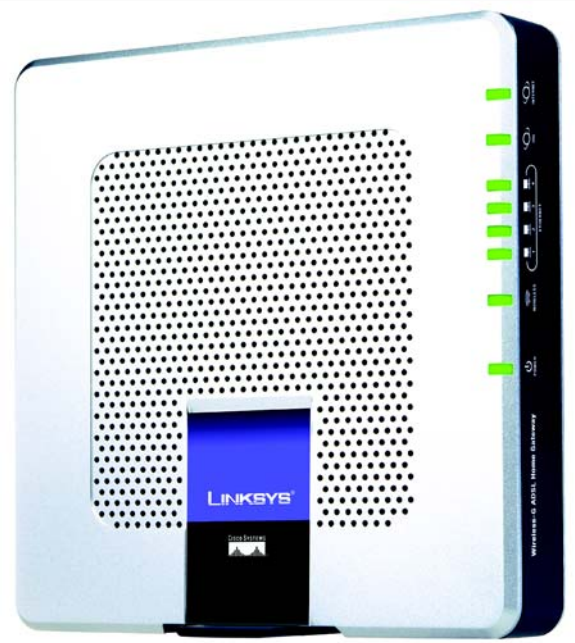
LINKSYS®
A Division of Cisco Systems, Inc.




2,4 GHz 802.11g **Wireless-G**

WIRELESS

ADSL-Home-Gateway **Benutzerhandbuch**

Modell-Nr. **WAG354G - Annex B (DE)**

CISCO SYSTEMS

## Copyright und Marken

Technische Änderungen vorbehalten. Linksys ist eine eingetragene Marke bzw. eine Marke von Cisco Systems, Inc. und/oder deren Zweigunternehmen in den USA und anderen Ländern. Copyright © 2005 Cisco Systems, Inc. Alle Rechte vorbehalten. Andere Handelsmarken und Produktnamen sind Marken bzw. eingetragene Marken der jeweiligen Inhaber.

## Hinweise zur Verwendung dieses Handbuchs

Ziel des Benutzerhandbuchs zum Wireless-G ADSL-Home-Gateway ist, Ihnen den Einstieg in den Netzwerkbetrieb mit dem Gateway noch weiter zu erleichtern. Achten Sie beim Lesen dieses Benutzerhandbuchs auf Folgendes:

Dieses Häkchen kennzeichnet einen Hinweis, den Sie bei Verwendung des Gateways besonders beachten sollten.

Dieses Ausrufezeichen kennzeichnet eine Warnung und weist darauf hin, dass unter bestimmten Umständen Schäden an Ihrem Eigentum oder am Gateway verursacht werden können.

Dieses Fragezeichen dient als Erinnerung an bestimmte Schritte, die bei Verwendung des Gateways durchzuführen sind.

Neben den Symbolen finden Sie Definitionen für technische Begriffe, die in folgender Form dargestellt werden:

***Begriff:*** *Definition.*

Alle Abbildungen (Diagramme, Bildschirmdarstellungen und andere Bilder) sind mit einer Abbildungsnummer und einer Kurzbeschreibung versehen (siehe folgendes Beispiel):

**Abbildung 0-1: Kurzbeschreibung der Abbildung**

Die Abbildungsnummern und die zugehörigen Kurzbeschreibungen finden Sie auch im Inhaltsverzeichnis unter „Abbildungsverzeichnis“.

# Inhaltsverzeichnis

Kapitel 1: Einführung 1
Willkommen 1
Inhalt dieses Benutzerhandbuchs 2
Kapitel 2: Planen Ihres Netzwerks 4
Die Funktionen des Gateways 4
IP-Adressen 4
Kapitel 3: Beschreibung des Wireless-G ADSL-Home-Gateways 6
Ports und Reset-Taste an der Seitenwand 6
LEDs an der Seitenwand 7
Untere Gehäusekante 8
Kapitel 4: Anschließen des Wireless-G ADSL-Home-Gateways 9
Übersicht 9
Verdrahtete Verbindung mit einem Computer 10
Wireless-Verbindung mit einem Computer 11
Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways 12
Übersicht 12
Hinweis für den Zugriff auf das webbasierte Dienstprogramm 14
Registerkarte „Setup“ (Einrichtung) 14
Registerkarte „Wireless“ 22
Registerkarte „Security“ (Sicherheit) 27
Registerkarte „Access Restrictions“ (Zugriffsbeschränkungen) 29
Registerkarte „Applications and Gaming“ (Anwendungen und Spiele) 31
Registerkarte „Administration“ (Verwaltung) 36
Registerkarte „Status“ 42
Anhang A: Fehlerbehebung 46
Behebung häufig auftretender Probleme 46
Häufig gestellte Fragen 56
Anhang B: Sicherheit im Wireless-Netzwerkbetrieb 63
Vorsichtsmaßnahmen 63
Sicherheitsrisiken bei Wireless-Netzwerken 63

Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters 66
Anweisungen für Windows 98/ME 66
Anweisungen für Windows 2000/XP 67
Anhang D: Aktualisieren der Firmware 68
Anhang E: Glossar 69
Anhang F: Zulassungsinformationen 77
Anhang G: Garantieinformationen 83
Anhang H: Spezifikationen 84
Anhang I: Kontaktinformationen 86

# Abbildungsverzeichnis

Abbildung 2-1: Netzwerk 4
Abbildung 3-1: Ports und Reset-Taste an der Seitenwand 6
Abbildung 3-2: LEDs an der Seitenwand 7
Abbildung 3-3: Untere Gehäusekante mit Ständer in geschlossener Position 8
Abbildung 3-4: Gateway mit verwendetem Ständer 8
Abbildung 4-1: Herstellen der ADSL-Verbindung 10
Abbildung 4-2: Anschließen eines PCs 10
Abbildung 4-3: Anschließen des Netzstroms 10
Abbildung 4-4: Herstellen der ADSL-Verbindung 11
Abbildung 4-5: Anschließen des Netzstroms 11
Abbildung 5-1: Anmeldefenster 14
Abbildung 5-2: Grundlegende Einrichtung 14
Abbildung 5-3: RFC 1483-Überbrückung - Dynamische IP-Adresse 15
Abbildung 5-4: RFC 1483-Überbrückung - Statische IP-Adresse 15
Abbildung 5-5: RFC 1483-Weiterleitung 16
Abbildung 5-6: RFC 2516 PPPoE 16
Abbildung 5-7: RFC 2364 PPPoA 17
Abbildung 5-8: Nur Überbrückungsmodus 17
Abbildung 5-9: Optionale Einstellungen 18
Abbildung 5-10: DynDNS.org 19
Abbildung 5-11: TZO.com 19
Abbildung 5-12: Erweitertes Routing 20
Abbildung 5-13: Routing-Tabelle 21
Abbildung 5-14: Grundlegende Wireless-Einstellungen 22
Abbildung 5-15: WPA Vorläufiger gemeinsamer Schlüssel 23
Abbildung 5-16: WEP 24
Abbildung 5-17: Wireless-Netzwerkzugriff 25
Abbildung 5-18: MAC-Adressen-Filterliste 25
Abbildung 5-19: MAC-Liste der Wireless-Clients 25
Abbildung 5-20: Erweiterte Wireless-Einstellungen 26
Abbildung 5-21: Sicherheit 27
Abbildung 5-22: Firewall-Protokoll 28

Abbildung 5-23: Internetzugriff 29
Abbildung 5-24: Internet-Richtlinien - Zusammenfassung 29
Abbildung 5-25: PC-Liste 30
Abbildung 5-26: Dienst hinzufügen/bearbeiten 30
Abbildung 5-27: Einfaches Port-Forwarding 31
Abbildung 5-28: Port Range Forwarding (Weiterleitung an einen Anschlussbereich) 32
Abbildung 5-29: Port-Triggering 33
Abbildung 5-30: DMZ 34
Abbildung 5-31: QoS 35
Abbildung 5-32: Verwaltungsfunktionen 36
Abbildung 5-33: Zugelassene IP bzw. zugelassener IP-Bereich 36
Abbildung 5-34: Berichtaufzeichnung 38
Abbildung 5-35: Systemprotokoll 38
Abbildung 5-36: Ping-Test 39
Abbildung 5-37: Sichern & Wiederherstellen 39
Abbildung 5-38: Werkseinstellungen 40
Abbildung 5-39: Firmware aktualisieren 40
Abbildung 5-40: Neustart 41
Abbildung 5-41: Gateway 42
Abbildung 5-42: Lokales Netzwerk 43
Abbildung 5-43: DHCP - Tabelle zur aktiven IP-Adresse 43
Abbildung 5-44: ARP/RARP-Tabelle 43
Abbildung 5-45: Wireless 44
Abbildung 5-46: Netzwerk-Computer 44
Abbildung 5-47: DSL-Verbindung 45
Abbildung C-1: Fenster „IP-Konfiguration“ 66
Abbildung C-2: MAC-Adresse/Adapteradresse 66
Abbildung C-3: MAC-Adresse/physikalische Adresse 67
Abbildung D-1: Firmware aktualisieren 68

# Kapitel 1: Einführung

## Willkommen

Vielen Dank, dass Sie sich für ein Wireless-G ADSL-Home-Gateway entschieden haben. Mit diesem Gateway stehen Ihren Computern eine High Speed-Internetverbindung und Ressourcen wie beispielsweise Dateien und Drucker zur Verfügung. Da es sich um ein Wireless-Gateway handelt, kann der Internetzugriff sowohl über das verdrahtete Netzwerk als auch als Wireless-Übertragung mit bis zu 11 Mbit/s für Wireless-B bzw. 54 Mbit/s für Wireless-G erfolgen.

Wie schafft das Gateway das? Wenn das Gateway mit dem Internet sowie Computern und Peripheriegeräten verbunden wird, kann die Netzwerkkommunikation durch das Gateway gesteuert und überwacht werden.

Das Gateway verfügt zum Schutz Ihrer Daten und Ihrer Privatsphäre über eine verbesserte Firewall, mit der Eindringlinge aus dem Internet abgewehrt werden. Wireless-Datenübertragungen können durch leistungsstarke Datenverschlüsselung geschützt werden. Zudem können Sie Ihre Familie mit Kinderschutzfunktionen wie dem Einschränken der Internetzugriffszeiten und dem Blockieren von Schlüsselwörtern schützen. Die Gateway-Einstellungen können über das benutzerfreundliche, browserbasierte Dienstprogramm konfiguriert werden.

Und was genau bedeutet das?

Mit Netzwerken können Sie einen Internetzugang und Computer-Ressourcen gemeinsam mit anderen nutzen. Sie können von verschiedenen Computern aus auf einem Drucker drucken und auf Daten zugreifen, die auf der Festplatte eines anderen Computers gespeichert sind. Netzwerke eignen sich darüber hinaus auch für Videospiele mit mehreren Spielern. Netzwerke sind also nicht nur zu Hause und im Büro nützlich, sondern lassen sich auch für Unterhaltungszwecke nutzen.

Mehrere PCs in einem verdrahteten Netzwerk stellen ein LAN (*Local Area Network*; Lokales Netzwerk) dar. Sie werden über Ethernetkabel angeschlossen, daher die Bezeichnung „verdrahtetes“ Netzwerk. Mit Wireless-Karten oder -Adaptern ausgerüstete PCs können ganz ohne lästige Kabel kommunizieren. Indem sie innerhalb ihres Übertragungsradius dieselben Wireless-Einstellungen verwenden, bilden sie ein Wireless-Netzwerk. Dies wird oft als WLAN (*Wireless Local Area Network*) oder drahtloses lokales Netzwerk bezeichnet. Da das Gateway mit Wireless-Funktionen ausgestattet ist, kann es verdrahtete Netzwerke und Wireless-Netzwerke miteinander verbinden, so dass diese miteinander kommunizieren können.

Durch das Verbinden aller verdrahteten und Wireless-Netzwerke sowie des Internets können Sie jetzt Dateien gemeinsam nutzen, gemeinsam auf das Internet zugreifen und sogar Spiele spielen. Und dabei schützt das Wireless-G ADSL-Home-Gateway Ihre Netzwerke stets vor nicht autorisierten und nicht willkommenen Benutzern.

Linksys empfiehlt, für die erstmalige Installation des Gateways die Installations-CD-ROM zu verwenden. Wenn Sie den auf der Installations-CD-ROM befindlichen Installationsassistenten nicht ausführen möchten, können Sie die in diesem Handbuch aufgeführten Anleitungsschritte durchführen, um das Gateway anzuschließen, einzurichten und für die Verbindung der verschiedenen Netzwerke zu konfigurieren. Diese Anleitungen enthalten alle Informationen, die Sie zur optimalen Nutzung des Wireless-G ADSL-Home-Gateways benötigen.

***WPA** (Wi-Fi Protected Access): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (Temporal Key Integrity Protocol) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann.*

***SPI-Firewall** (Stateful Packet Inspection): Eine Technologie zur Überprüfung von eingehenden Datenpaketen, bevor diese an das Netzwerk weitergeleitet werden.*

***Firewall**: Sicherheitsmaßnahmen, durch die die Ressourcen in einem lokalen Netzwerk vor dem Zugriff durch nicht autorisierte Dritte geschützt werden.*

***NAT** (Network Address Translation): Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.*

***Netzwerk:** Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam nutzen, speichern und untereinander übertragen können.*

***LAN** (Local Area Network): Die Computer und Netzwerkbetriebsprodukte, aus denen sich Ihr Heim- oder Büronetzwerk zusammensetzt.*

# Inhalt dieses Benutzerhandbuchs

In diesem Benutzerhandbuch sind die zur Installation und Verwendung des Wireless-G ADSL-Home-Gateways erforderlichen Schritte aufgeführt.

- Kapitel 1: Einführung
  In diesem Kapitel werden die Anwendungen des Wireless-G ADSL-Home-Gateways sowie dieses Benutzerhandbuch beschrieben.

- Kapitel 2: Planen Ihres Netzwerks
  In diesem Kapitel werden die Grundlagen des Netzwerkbetriebs beschrieben.

- Kapitel 3: Beschreibung des Wireless-G ADSL-Home-Gateways
  In diesem Kapitel werden die physischen Merkmale des Gateways beschrieben.

- Kapitel 4: Anschließen des Wireless-G ADSL-Home-Gateways
  In diesem Kapitel finden Sie Anleitungen zum Anschließen des Gateways an das Netzwerk.

- Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways
  In diesem Kapitel wird erläutert, wie Sie die Einstellungen des Gateways mithilfe des webbasierten Dienstprogramms konfigurieren.

- Anhang A: Fehlerbehebung
  In diesem Anhang werden einige Probleme und Lösungsansätze sowie häufig gestellte Fragen im Zusammenhang mit der Installation und Verwendung des Wireless-G ADSL-Home-Gateways erörtert.

- Anhang B: Sicherheit im Wireless-Netzwerkbetrieb
  In diesem Anhang werden die Risiken des Wireless-Netzwerkbetriebs sowie einige Lösungen zur Eingrenzung der Risiken erklärt.

- Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters
  In diesem Anhang wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterung bzw. die Gateway-Funktion zum Kopieren von MAC-Adressen verwenden zu können.

- Anhang D: Aktualisieren der Firmware
  In diesem Anhang finden Sie eine Anleitung zum Aktualisieren der Gateway-Firmware, sollte dies einmal erforderlich sein.

- Anhang E: Glossar
  In diesem Anhang finden Sie ein kurzes Glossar mit häufig verwendeten Begriffen aus dem Bereich Netzwerkbetrieb.

- Anhang F: Zulassungsinformationen
  In diesem Anhang sind die für das Gateway geltenden Zulassungsinformationen aufgeführt.

- Anhang G: Garantieinformationen
  Dieser Anhang enthält die Garantieinformationen für das Gateway.

- Anhang H: Spezifikationen
  In diesem Anhang sind die technischen Spezifikationen des Gateways aufgeführt.

- Anhang I: Kontaktinformationen
  In diesem Anhang finden Sie Kontaktinformationen zu einer Reihe von Linksys Ressourcen, darunter auch zum Kundendienst.

# Kapitel 2: Planen Ihres Netzwerks

## Die Funktionen des Gateways

Ein Gateway ist ein Netzwerkgerät, das zwei Netzwerke miteinander verbindet.

In diesem Fall verbindet das Gateway Ihr lokales Netzwerk (LAN) oder die Computer zu Hause oder im Büro mit dem Internet. Das Gateway verarbeitet und lenkt die zwischen diesen beiden Netzwerken übertragenen Daten.

Mit der NAT-Funktion des Gateways wird Ihr Computernetzwerk geschützt, so dass Ihre Computer für andere Benutzer im Internet nicht „sichtbar" sind. Somit wird der private Charakter Ihres Netzwerks bewahrt. Das Gateway schützt Ihr Netzwerk, indem es alle über den Internetanschluss eingehenden Datenpakete überprüft, bevor sie an den entsprechenden Computer in Ihrem Netzwerk geliefert werden. Das Gateway überprüft Internet-Anschlussdienste, wie z. B. den Webserver, FTP-Server oder andere Internetanwendungen, und leitet, sofern zulässig, das jeweilige Paket an den entsprechenden Computer im LAN weiter.

Beachten Sie, dass Sie über die Ports des Gateways eine Verbindung zu zwei verschiedenen Netzwerken herstellen können. Mit den LAN-Ports können Sie eine Verbindung zum LAN und mit dem ADSL-Port eine Verbindung zum Internet herstellen. Die LAN-Ports übertragen Daten mit einer Geschwindigkeit von 10/100 Mbit/s.

**Abbildung 2-1: Netzwerk**

## IP-Adressen

### Was ist eine IP-Adresse?

IP steht für *Internet Protocol* (Internet Protokoll). Jedes Gerät in einem IP-basierten Netzwerk, einschließlich Computern, Druckservern und Gateways, benötigt eine IP-Adresse, mit der sein „Standpunkt" bzw. seine Adresse im Netzwerk identifiziert werden kann. Dies gilt sowohl für Internet- als auch für LAN-Verbindungen. Es gibt zwei Möglichkeiten, Ihren Netzwerkgeräten eine IP-Adresse zuzuweisen. Sie können statische IP-Adressen oder mithilfe des Gateways dynamische IP-Adressen zuweisen.

***IP** (Internet Protocol): Ein Protokoll, mit dem Daten über Netzwerke gesendet werden.*

**HINWEIS:** Da es sich bei dem Gateway um ein Gerät handelt, mit dem zwei Netzwerke verbunden werden, sind zwei IP-Adressen erforderlich, eine für das LAN und eine für das Internet. In diesem Benutzerhandbuch wird auf „Internet-IP-Adressen" und „LAN-IP-Adressen" verwiesen.

### Statische IP-Adressen

Bei einer statischen IP-Adresse handelt es sich um eine feste IP-Adresse, die einem Computer oder einem anderen Netzwerkgerät manuell zugewiesen wird. Da eine statische IP-Adresse solange gültig ist, bis Sie sie deaktivieren, wird durch das Zuweisen einer statischen IP-Adresse sichergestellt, dass das entsprechende Gerät stets dieselbe IP-Adresse hat, bis diese geändert wird. Statische IP-Adressen müssen eindeutig sein und werden im Allgemeinen bei Netzwerkgeräten, wie z. B. Server-Computern oder Druckservern, verwendet.

Da bei dem Gateway NAT-Technologie eingesetzt wird, ist die einzige IP-Adresse Ihres Netzwerks, die vom Internet aus sichtbar ist, die Internet-IP-Adresse des Gateways. Es kann jedoch auch diese Internet-IP-Adresse blockiert werden, so dass Gateway und Netzwerk für das Internet unsichtbar sind. Weitere Informationen hierzu finden Sie in „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways" unter „Sicherheit" in der Beschreibung zum Blockieren von WAN-Anfragen.

Da Sie das Gateway für den gemeinsamen Zugriff auf Ihre DSL-Internetverbindung verwenden, fragen Sie Ihren ISP, ob Ihrem Konto eine statische IP-Adresse zugewiesen wurde. Ist dies der Fall, benötigen Sie diese statische IP-Adresse für die Konfiguration des Gateways. Sie erhalten diese Informationen von Ihrem ISP.

## Dynamische IP-Adressen

Eine dynamische IP-Adresse wird einem Netzwerkgerät, wie z. B. einem Computer oder Druckserver, automatisch zugewiesen. Diese IP-Adressen werden als „dynamisch“ bezeichnet, da sie den Netzwerkgeräten nur vorübergehend zugewiesen werden. Nach einem bestimmten Zeitraum laufen Sie ab und können geändert werden. Wenn ein Computer beim Netzwerk (oder im Internet) angemeldet wird und seine dynamische IP-Adresse abgelaufen ist, wird ihm vom DHCP-Server automatisch eine neue dynamische IP-Adresse zugewiesen.

## DHCP-Server (*Dynamic Host Configuration Protocol*)

Computern und anderen Netzwerkgeräten mit dynamischen IP-Adressen wird von einem DHCP-Server jeweils eine neue IP-Adresse zugewiesen. Computer bzw. Netzwerkgeräte, die eine IP-Adresse erhalten, werden als DHCP-Clients bezeichnet. Durch DHCP müssen Sie nicht jedes Mal, wenn dem Netzwerk ein neuer Benutzer hinzugefügt wird, manuell eine IP-Adresse zuweisen.

Als DHCP-Server kann entweder ein bestimmter Computer im Netzwerk oder ein anderes Netzwerkgerät, wie z. B. das Gateway, fungieren. Die DHCP-Serverfunktion des Gateways ist standardmäßig aktiviert.

Wenn in Ihrem Netzwerk bereits ein DHCP-Server ausgeführt wird, müssen Sie einen der beiden DHCP-Server deaktivieren. Wenn mehr als ein DHCP-Server in Ihrem Netzwerk ausgeführt werden, treten Netzwerkfehler, wie z. B. IP-Adresskonflikte, auf. Informationen zum Deaktivieren der DHCP-Funktion beim Gateway erhalten Sie in „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“.

# Kapitel 3: Beschreibung des Wireless-G ADSL-Home-Gateways

## Ports und Reset-Taste an der Seitenwand

Die Ports und die Reset-Taste des Gateways befinden sich an der Seitenwand.

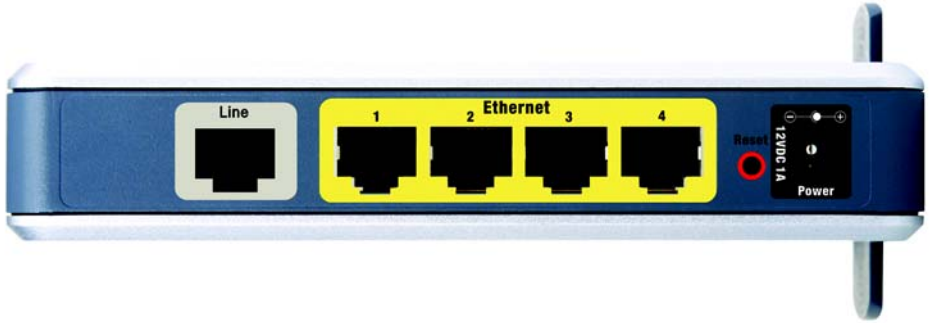



**Abbildung 3-1: Ports und Reset-Taste an der Seitenwand**

**Line** (Verbindung) Der **Line**-Port dient zum Anschließen an die ADSL-Verbindung.

**Ethernet (1-4)** Die **Ethernet**-Ports dienen zum Anschließen an die Computer und andere Netzwerkgeräte.

**Reset-Taste** Das Gateway kann auf zweierlei Weise auf die Werkseinstellungen zurückgesetzt werden. Halten Sie entweder die **Reset-Taste** ungefähr zehn Sekunden lang gedrückt, oder setzen Sie die Einstellungen im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Administration** (Verwaltung) unter **Factory Defaults** (Werkseinstellungen) zurück.

**Power** (Netzstrom) Der **Power**-Port dient zum Anschließen des Netzstromadapters.

**WICHTIG:** Durch das Zurücksetzen des Gateways auf die Werkseinstellungen werden alle Einstellungen gelöscht (einschließlich der Einstellungen für die Internetverbindung, der Wireless-Einstellungen und anderer Einstellungen) und durch die Werkseinstellungen ersetzt. Wenn Sie diese Einstellungen beibehalten möchten, sollten Sie das Gateway nicht zurücksetzen.

# LEDs an der Seitenwand

Die LEDs des Gateways, die Netzwerkaktivität anzeigen, befinden sich an der anderen Seitenwand.

**Abbildung 3-2: LEDs an der Seitenwand**

| | |
|---|---|
| **POWER** (Netzstrom) | Grün. Die **POWER**-LED leuchtet auf, wenn das Gateway eingeschaltet wird. |
| **WIRELESS** | Grün. Die **WIRELESS**-LED leuchtet bei jeder erfolgreichen Wireless-Verbindung auf. Wenn die LED blinkt, werden gerade aktiv Daten vom Gateway an eines der Netzwerkgeräte gesendet oder es werden gerade Daten empfangen. |
| **ETHERNET (1-4)** | Grün. Die **ETHERNET**-LED hat zwei Funktionen. Wenn die LED durchgängig leuchtet, ist das Gateway erfolgreich über den LAN-Port mit einem Gerät verbunden. Wenn die LED blinkt, finden Netzwerkaktivitäten statt. |
| **DSL** | Grün. Die **DSL-**LED leuchtet bei jeder erfolgreichen DSL-Verbindung auf. Wenn das Gateway eine ADSL-Verbindung herstellt, blinkt die LED. |
| **INTERNET** | Grün. Die **INTERNET**-LED leuchtet grün auf, wenn eine Internetverbindung zum Internet-Dienstanbieters (ISP) hergestellt wurde. Die **INTERNET**-LED leuchtet rot auf, wenn die Verbindung zum ISP fehlgeschlagen ist. |

## Untere Gehäusekante

Das Gateway verfügt über einen integrierten Ständer. Wenn Sie das Gateway flach hinlegen möchten, kann der Ständer in geschlossener Position bleiben. Wenn Sie das Gateway jedoch aufrecht hinstellen möchten, drehen Sie den Ständer um 90 º im Uhrzeigersinn und bringen Sie das Gateway in die gewünschte Position.

**Abbildung 3-3: Untere Gehäusekante mit Ständer in geschlossener Position**

**Abbildung 3-4: Gateway mit verwendetem Ständer**

# Kapitel 4: Anschließen des Wireless-G ADSL-Home-Gateways

## Übersicht

In der Regel erhalten Sie vom Installationstechniker Ihres Internet-Dienstanbieters (ISP) nach der Installation der Breitbandverbindung Informationen zur Einrichtung des Modems. Wenn diese Daten nicht zur Verfügung stehen, fordern Sie sie von Ihrem ISP an.

Wenn Sie über die für Ihren Internetverbindungstyp erforderlichen Einrichtungsinformationen verfügen, können Sie mit der Installation und der Einrichtung des Gateways beginnen.

Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Ethernet-Adapter verwenden möchten, fahren Sie mit dem Abschnitt „Verdrahtete Verbindung mit einem Computer“ fort. Wenn Sie zur Konfiguration des Gateways einen Computer mit einem Wireless-Adapter verwenden möchten, fahren Sie mit dem Abschnitt „Wireless-Verbindung mit einem Computer“ fort.

# Verdrahtete Verbindung mit einem Computer

1. Stellen Sie sicher, dass alle Hardwaregeräte des Netzwerks (einschließlich des Gateways und der Computer) ausgeschaltet sind.
2. Schließen Sie ein Ende des Ethernet-Kabels (KAT5) an den Line-Port, der sich an der Rückseite des Gateways befindet, und das andere Ende an den NTBA an.

   **WICHTIG:** Benutzer von Annex B (Gateway-Versionen E1 und DE) verwenden zum Anschließen des Gateways an die Wandbuchse das im Lieferumfang enthaltene Kabel.
   Wenn Sie Splitter oder spezielle Stecker benötigen, wenden Sie sich an Ihren Internet-Dienstanbieter.

3. Schließen Sie ein Ende des Ethernet-Netzwerkkabels an einen der Ethernet-Ports (mit 1-4 beschriftet) an der Seitenwand des Gateways und das andere Ende am Ethernet-Port eines Computers an.

   Wiederholen Sie diesen Schritt, um weitere Computer, einen Switch oder andere Netzwerkgeräte an das Gateway anzuschließen.
4. Schließen Sie das Netzteil an den Netzstrom-Port des Gateways an, und stecken Sie das Netzteil anschließend in eine Steckdose.

   **HINWEIS:** Schließen Sie das Netzteil des Gateways nur an eine Stromleiste mit Überspannungsschutz an.

   Wenn das Netzteil richtig angeschlossen ist, leuchtet die Netzstrom-LED an der Seitenwand grün. Die Netzstrom-LED blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen wurde. Wenn die LED eine Minute oder länger blinkt, finden Sie in „Anhang A: Fehlerbehebung“ entsprechende Informationen.
5. Schalten Sie einen Computer ein, der mit dem Gateway verbunden ist.

**Fahren Sie mit „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“ fort.**

**Abbildung 4-1: Herstellen der ADSL-Verbindung**

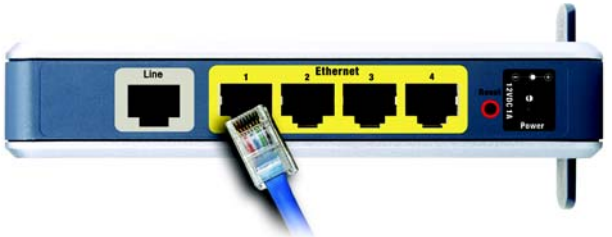



**Abbildung 4-2: Anschließen eines PCs**

**Abbildung 4-3: Anschließen des Netzstroms**

## Wireless-Verbindung mit einem Computer

Befolgen Sie diese Anweisungen, wenn Sie über eine Wireless-Verbindung auf das Gateway zugreifen möchten:

1. Stellen Sie sicher, dass alle Hardwaregeräte des Netzwerks (einschließlich des Gateways und der Computer) ausgeschaltet sind.
2. Schließen Sie ein Ende des Ethernet-Kabels (KAT5) an den Line-Port auf der Rückseite des Gateways und das andere Ende an den NTBA an.

**WICHTIG:** Benutzer von Annex B (Gateway-Versionen E1 und DE) verwenden zum Anschließen des Gateways an die Wandbuchse das im Lieferumfang enthaltene Kabel. Wenn Sie Splitter oder spezielle Stecker benötigen, wenden Sie sich an Ihren Internet-Dienstanbieter.

3. Schließen Sie das Netzteil an den Netzstrom-Port an, und stecken Sie ihn anschließend in eine Steckdose.

   Wenn das Netzteil richtig angeschlossen ist, leuchtet die Netzstrom-LED an der Seitenwand grün. Die Netzstrom-LED blinkt einige Sekunden lang und leuchtet konstant, nachdem die Selbstdiagnose abgeschlossen wurde. Wenn die LED eine Minute oder länger blinkt, finden Sie in „Anhang A: Fehlerbehebung“ entsprechende Informationen.
4. Schalten Sie einen der Computer in Ihrem Wireless-Netzwerk ein.
5. Stellen Sie beim erstmaligen Zugriff auf das Gateway über eine Wireless-Verbindung sicher, dass die SSID des Wireless-Adapters des Computers auf **linksys** (die Standardeinstellung des Gateways) eingestellt und die Option zur Sicherheit im Wireless-Netzwerkbetrieb deaktiviert ist. Wenn Sie Zugriff auf das Gateway haben, können Sie die Einstellungen des Gateways und des Adapters dieses Computers an die üblichen Netzwerkeinstellungen anpassen.

**Fahren Sie mit „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“ fort.**

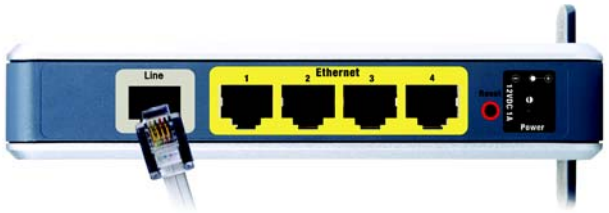



**Abbildung 4-4: Herstellen der ADSL-Verbindung**

**Abbildung 4-5: Anschließen des Netzstroms**

**HINWEIS:** Sie sollten stets die SSID-Standardeinstellung **linksys** ändern und die Option zur Sicherheit im Wireless-Netzwerkbetrieb aktivieren.

# Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways

## Übersicht

Folgen Sie zum Konfigurieren des Gateways den in diesem Kapitel aufgeführten Schritten, und verwenden Sie das webbasierte Dienstprogramm des Gateways. In diesem Kapitel werden alle Webseiten des Dienstprogramms und deren Hauptfunktionen beschrieben. Sie können das Dienstprogramm mit einem an das Gateway angeschlossenen Computer über Ihren Web-Browser aufrufen. Bei der grundlegenden Netzwerkeinrichtung verwenden die meisten Benutzer die folgenden Fenster des Dienstprogramms:

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie im Fenster **Basic Setup** (Grundlegende Einrichtung) die von Ihrem ISP bereitgestellten Einstellungen ein.
- **Management** (Verwaltungsfunktionen): Klicken Sie auf die Registerkarte **Administration** (Verwaltung) und anschließend auf die Registerkarte **Management** (Verwaltungsfunktionen). Der Standardbenutzername und das Standardpasswort des Gateways lauten **admin**. Ändern Sie das Standardpasswort, um das Gateway zu schützen.

Es gibt sieben Hauptregisterkarten: **Setup** (Einrichtung), **Wireless** (Wireless), **Security** (Sicherheit), **Access Restrictions** (Zugriffsbeschränkungen), **Applications & Gaming** (Anwendungen & Spiele) und **Status** (Status). Wenn Sie auf eine der Hauptregisterkarten klicken, sind jeweils zusätzliche Registerkarten verfügbar.

### Setup (Einrichtung)

- **Basic Setup** (Grundlegende Einrichtung): Geben Sie in dieses Fenster die Internetverbindung und die Netzwerkeinstellungen ein.
- **DDNS**: Füllen Sie die Felder dieses Fensters aus, um die Funktion **DDNS** (*Dynamic Domain Name System*) des Gateways zu aktivieren.
- **Advanced Routing** (Erweitertes Routing): In diesem Fenster können Sie die Konfigurationseinstellungen für NAT und Routing ändern.

### Wireless

- **Basic Wireless Settings** (Grundlegende Wireless-Einstellungen): In diesem Fenster können Sie die Wireless-Netzwerkeinstellungen auswählen.
- **Wireless Security** (Sicherheit im Wireless-Netzwerkbetrieb): Konfigurieren Sie in diesem Fenster die Wireless-Sicherheitseinstellungen.
- **Wireless Access** (Wireless-Zugriff): In diesem Fenster können Sie den Zugriff auf das Wireless-Netzwerk steuern.
- **Advanced Wireless Settings** (Erweiterte Wireless-Einstellungen): Über dieses Fenster können Sie auf die erweiterten Wireless-Netzwerkeinstellungen zugreifen.

**HABEN SIE:** TCP/IP auf den Computern aktiviert? Computer tauschen mit diesem Protokoll über das Netzwerk Daten aus. Weitere Informationen zu TCP/IP erhalten Sie in der Windows-Hilfe.

**HINWEIS:** Für zusätzliche Sicherheit sollten Sie das Passwort über die Registerkarte **Administration** (Verwaltung) ändern.

## Security (Sicherheit)

In diesem Fenster können Sie die Firewall deaktivieren bzw. aktivieren, Filter einrichten, WAN-Anfragen blockieren und VPN-Passthrough (*Virtual Private Networks*) aktivieren bzw. deaktivieren.

***VPN** (Virtual Private Network): Sicherheitsmaßnahme, mit der Daten geschützt werden, wenn sie über das Internet von einem Netzwerk in ein anderes übertragen werden.*

## Access Restrictions (Zugriffsbeschränkungen)

- **Internet Access** (Internetzugriff): In diesem Fenster können Sie die Internetverwendung und den Datenverkehr im lokalen Netzwerk steuern.

## Applications & Gaming (Anwendungen & Spiele)

- **Single Port Forwarding** (Einfaches Port-Forwarding): In diesem Fenster können Sie gängige Dienste oder Anwendungen einrichten, für die das Weiterleiten eines einzelnen Ports erforderlich ist.
- **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich): In diesem Fenster können Sie öffentliche Dienste oder andere spezielle Internetanwendungen einrichten, für die das Weiterleiten eines Anschlussbereichs erforderlich ist.
- **Port Triggering** (Port-Triggering): Klicken Sie auf diese Registerkarte, um die Bereiche für Port-Triggering und Port-Forwarding für Internet-Anwendungen festzulegen.
- **DMZ**: Richten Sie in diesem Fenster die Internetverbindung für einen lokalen Computer so ein, dass spezielle Dienste verwendet werden können.
- **QoS:** Ordnen Sie mit QoS (*Quality of Service*) unterschiedliche Arten der Datenübertragung verschiedenen Prioritätsstufen zu.

## Administration (Verwaltung)

- **Management** (Verwaltungsfunktionen): In diesem Fenster können Sie die Einstellungen für den Gateway-Zugriff, für SNMP (*Simple Network Management Protocol* ), UPnP (*Universal Plug and Play*), IGMP-Proxy (IGMP ist die Abkürzung für *Internet Group Multicast Protocol*) und für die Wireless-Verwaltung ändern.
- **Reporting** (Berichtaufzeichnung): Klicken Sie auf diese Registerkarte, um Aktivitätsprotokolle anzuzeigen oder zu speichern.
- **Diagnostics** (Diagnose): In diesem Fenster können Sie Ping-Tests ausführen.
- **Backup & Restore** (Sichern & Wiederherstellen): In diesem Fenster können Sie die Konfiguration des Gateways sichern und wiederherstellen.
- **Factory Defaults** (Werkseinstellungen): Verwenden Sie dieses Fenster, wenn Sie die Werkseinstellungen des Gateways wiederherstellen möchten.
- **Firmware Upgrade** (Firmware aktualisieren): Klicken Sie auf diese Registerkarte, um die Gateway-Firmware zu aktualisieren.
- **Reboot** (Neustart): In diesem Fenster können Sie einen Warm- oder Kaltstart des Gateways ausführen.

### Status

- **Gateway**: In diesem Fenster sind die Statusinformationen des Gateways aufgeführt.
- **Local Network** (Lokales Netzwerk): In diesem Fenster sind die Statusinformationen des lokalen Netzwerks aufgeführt.
- **Wireless** (Wireless-Netzwerk): In diesem Fenster sind die Statusinformationen des Wireless-Netzwerks aufgeführt.
- **DSL Connection** (DSL-Verbindung): In diesem Fenster sind die Statusinformationen der DSL-Verbindung aufgeführt.

## Hinweis für den Zugriff auf das webbasierte Dienstprogramm

Um auf das webbasierte Dienstprogramm zuzugreifen, starten Sie Internet Explorer oder Netscape Navigator und geben Sie im Feld *Adresse* die Standard-IP-Adresse des Gateways (**192.168.1.1**) ein. Drücken Sie anschließend die Eingabetaste.

Daraufhin wird ein Anmeldefenster angezeigt. (Unter Windows XP wird ein ähnliches Fenster angezeigt.) Geben Sie **admin** (als Standardbenutzername) in das Feld *Benutzername* sowie **admin** (als Standardkennwort) in das Feld *Kennwort* ein. Klicken Sie anschließend auf die Schaltfläche **OK**.

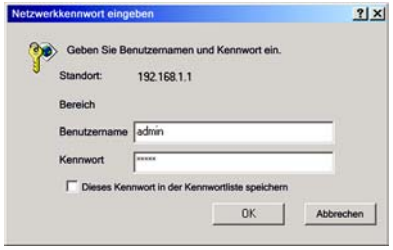



**Abbildung 5-1: Anmeldefenster**

## Registerkarte „Setup“ (Einrichtung)

### Registerkarte „Basic Setup“ (Grundlegende Einrichtung)

Im ersten dargestellten Fenster wird die Registerkarte **Basic Setup** (Grundlegende Einrichtung) angezeigt. Auf dieser Registerkarte können Sie die allgemeinen Einstellungen des Gateways ändern. Ändern Sie diese Einstellungen wie hier beschrieben, und klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Änderungen zu übernehmen, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen zu verwerfen.

#### Internet-Einrichtung

- **Internet Connection Type** (Internet-Verbindungstyp): Das Gateway unterstützt fünf Kapselungstypen: **RFC 1483 Bridged** (RFC 1483-Überbrückung), **RFC 1483 Routed** (RFC 1483-Weiterleitung), **RFC 2516 PPPoE**, **RFC 2364 PPPoA** und **Bridged Mode Only** (Nur Überbrückungsmodus). Wählen Sie aus dem Dropdown-Menü den geeigneten Kapselungstyp aus. Das jeweilige Fenster *Basic Setup* (Grundlegende Einrichtung) und die verfügbaren Funktionen unterscheiden sich je nach ausgewähltem Kapselungstyp.
- **VC Settings** (VC-Einstellungen): In diesem Bereich können Sie die VC-Einstellungen (*Virtual Circuit* ) konfigurieren.
  - **Multiplexing**: Wählen Sie je nach ISP **LLC** (LLC-Multiplexing) oder **VC** (VC-Multiplexing) aus.
  - **QoS Type** (QoS-Typ): Wählen Sie im Dropdown-Menü aus den folgenden Optionen aus: **CBR** (*Continuous Bit Rate;* Konstante Bitrate), um eine feste Bandbreite für Sprach- oder Datenverkehr festzulegen, **UBR** (*Unspecific Bit Rate*; Unbestimmte Bitrate) für Anwendungen, die zeitunabhängig sind (z. B. E-Mail), oder **VBR** (*Variable Bit Rate*; Variable Bitrate) für diskontinuierlichen Verkehr und Bandbreiten, die mit anderen Anwendungen gemeinsam genutzt werden.

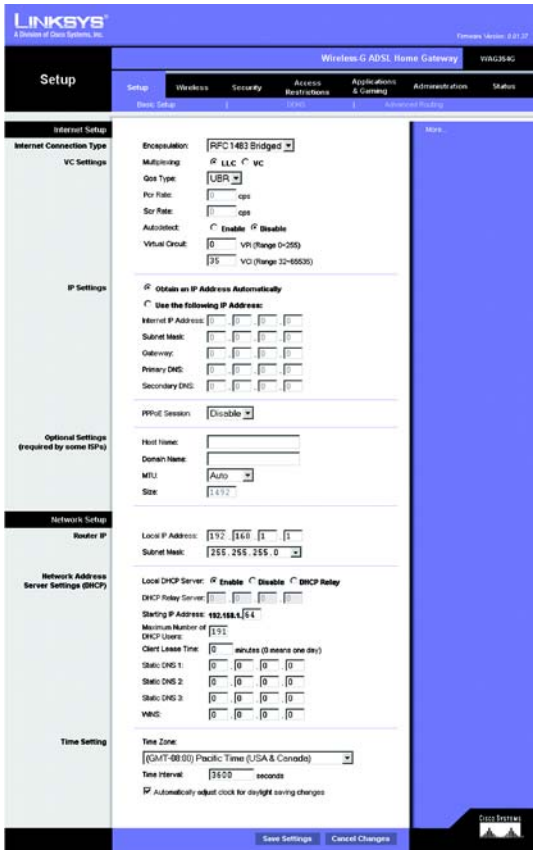



**Abbildung 5-2: Grundlegende Einrichtung**

- **PCR Rate** (PCR-Rate): Wenn Sie die Rate der DSL-Leitung durch 424 dividieren, erhalten Sie die PCR-Rate, anhand der Sie die maximale Rate, mit der der Absender Zellen senden kann, feststellen können. Geben Sie die Rate in das Feld ein (sofern Ihr Dienstanbieter dies erfordert).

- **SCR Rate** (SCR-Rate): Bestimmt den Mittelwert der Zellrate, die übertragen werden kann. Der Wert der SCR-Rate liegt gewöhnlich unter dem Wert der PCR-Rate. Geben Sie die Rate in das Feld ein (sofern Ihr Dienstanbieter dies erfordert).

- **Autodetect** (Automatisch erkennen): Wählen Sie **Enable** (Aktivieren) aus, damit die Einstellungen automatisch eingegeben werden, oder **Disable** (Deaktivieren), um die Werte manuell einzugeben.

- Virtueller Kreis: Für diese Felder gibt es zwei Optionen: **VPI** (*Virtual Path Identifier*; Virtueller Pfadidentifizierer) und **VCI** (*Virtual Channel Identifier*; Virtueller Kanalidentifizierer). Die korrekten Einstellungen erhalten Sie von Ihrem ISP.

- **IP Settings** (IP-Einstellungen): Befolgen Sie die Anweisungen, die im Abschnitt für den von Ihnen verwendeten Kapselungstyp aufgeführt sind.

## RFC 1483-Überbrückung

### Dynamische IP-Adresse

**IP Settings** (IP-Einstellungen): Wählen Sie **Obtain an IP Address Automatically** (IP-Adresse automatisch beziehen), wenn Sie laut Angaben Ihres ISP die Verbindung über eine dynamische IP-Adresse herstellen.

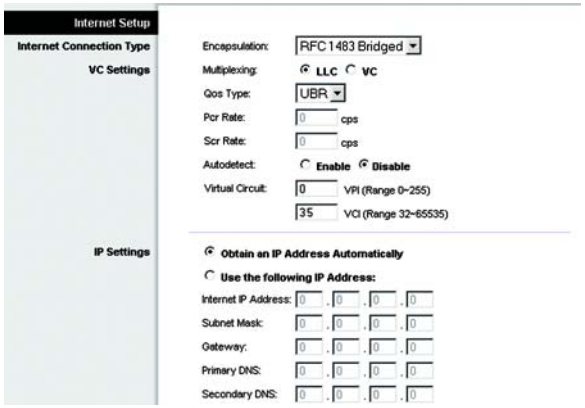

Internet Setup
Internet Connection Type
VC Settings
Encapsulation: RFC 1483 Bridged
Multiplexing: LLC VC
Qos Type: UBR
Pcr Rate: 0 cps
Scr Rate: 0 cps
Autodetect: Enable Disable
Virtual Circuit: 0 VPI (Range 0~255)
35 VCI (Range 32~65535)
IP Settings
Obtain an IP Address Automatically
Use the following IP Address:
Internet IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Gateway: 0 . 0 . 0 . 0
Primary DNS: 0 . 0 . 0 . 0
Secondary DNS: 0 . 0 . 0 . 0

**Abbildung 5-3: RFC 1483-Überbrückung - Dynamische IP-Adresse**

### Statische IP-Adresse

Wenn Sie für die Internetverbindung eine permanente (statische) IP-Adresse verwenden, wählen Sie **Use the following IP Address** (Folgende IP-Adresse verwenden) aus.

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.

- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.

- **Gateway**: Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.

- **Primary DNS** (Primärer DNS; erforderlich) und **Secondary DNS** (Sekundärer DNS; optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

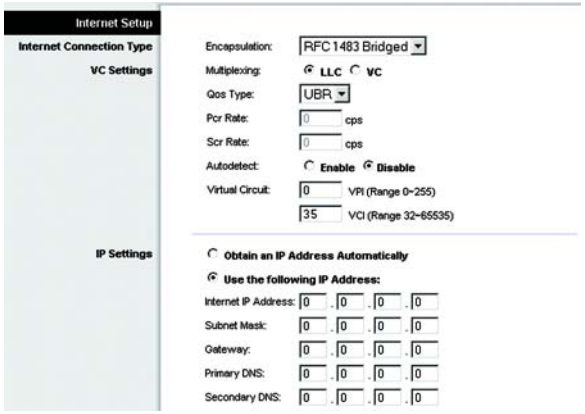

Internet Setup
Internet Connection Type
VC Settings
Encapsulation: RFC 1483 Bridged
Multiplexing: LLC VC
Qos Type: UBR
Pcr Rate: 0 cps
Scr Rate: 0 cps
Autodetect: Enable Disable
Virtual Circuit: 0 VPI (Range 0~255)
35 VCI (Range 32~65535)
IP Settings
Obtain an IP Address Automatically
Use the following IP Address:
Internet IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Gateway: 0 . 0 . 0 . 0
Primary DNS: 0 . 0 . 0 . 0
Secondary DNS: 0 . 0 . 0 . 0

**Abbildung 5-4: RFC 1483-Überbrückung - Statische IP-Adresse**

## RFC 1483-Weiterleitung

Wählen Sie zur Verwendung des Modus **RFC 1483 Routed** (RFC 1483-Weiterleitung) die Option **RFC 1483 Routed** (RFC 1483-Weiterleitung) aus.

- **Internet IP Address** (Internet-IP-Adresse): Hierbei handelt es sich um die IP-Adresse des Gateways, vom Standpunkt des WAN bzw. des Internets aus gesehen. Sie erhalten die hier anzugebene IP-Adresse von Ihrem ISP.
- **Subnet Mask** (Subnetzmaske): Hierbei handelt es sich um die Subnetzmaske des Gateways. Sie erhalten die Subnetzmaske von Ihrem ISP.
- **Gateway**: Sie erhalten die Standard-Gateway-Adresse von Ihrem ISP. Bei dieser Adresse handelt es sich um die IP-Adresse des ISP-Servers.
- **Primary DNS** (Primärer DNS; erforderlich) und **Secondary DNS** (Sekundärer DNS; optional): Sie erhalten von Ihrem ISP mindestens eine Server-IP-Adresse für das DNS (*Domain Name System*).

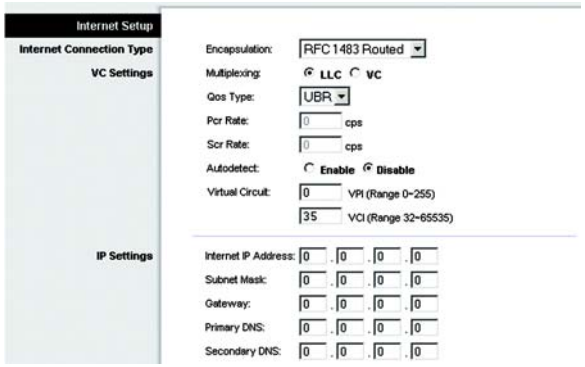

Internet Setup
Internet Connection Type
VC Settings
Encapsulation: RFC 1483 Routed
Multiplexing: LLC VC
Qos Type: UBR
Pcr Rate: 0 cps
Scr Rate: 0 cps
Autodetect: Enable Disable
Virtual Circuit: 0 VPI (Range 0~255)
35 VCI (Range 32~65535)
IP Settings
Internet IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Gateway: 0 . 0 . 0 . 0
Primary DNS: 0 . 0 . 0 . 0
Secondary DNS: 0 . 0 . 0 . 0

**Abbildung 5-5: RFC 1483-Weiterleitung**

## RFC 2516 PPPoE

Einige ISPs auf DSL-Basis verwenden PPPoE (*Point-to-Point Protocol over Ethernet*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Verbindung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoE verwendet wird. Falls ja, aktivieren Sie die Option **PPPoE**.

- **Service Name** (Dienstname): Geben Sie den Namen Ihres PPPoE-Diensts in dieses Feld ein.
- **User Name** (Benutzername) und **Password** (Passwort): Geben Sie den Benutzernamen und das Passwort ein (von Ihrem ISP bereitgestellt).
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Connect on Demand** (Bei Bedarf verbinden). Geben Sie im Feld *Max Idle Time* (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (Verbindung aufrechterhalten: Wahlwiederholung): Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Keep Alive** (Verbindung aufrechterhalten). Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Standardmäßig erfolgt die Wahlwiederholung nach **20** Sekunden.

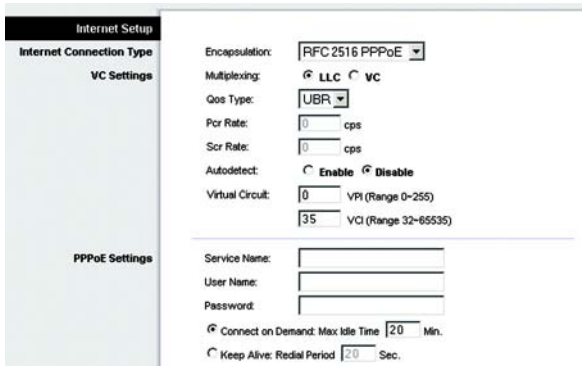



**Abbildung 5-6: RFC 2516 PPPoE**

## RFC 2364 PPPoA

Einige ISPs auf DSL-Basis verwenden PPPoA (*Point-to-Point Protocol over ATM*) zur Herstellung von Internetverbindungen. Wenn Sie über eine DSL-Leitung mit dem Internet verbunden sind, klären Sie mit Ihrem ISP, ob PPPoA verwendet wird. Falls ja, aktivieren Sie die Option **PPPoA**.

- **User Name** (Benutzername) und **Password** (Passwort): Geben Sie den Benutzernamen und das Passwort ein (von Ihrem ISP bereitgestellt).
- **Connect on Demand: Max Idle Time** (Bei Bedarf verbinden: Max. Leerlaufzeit): Sie können das Gateway so konfigurieren, dass die Internetverbindung nach einem bestimmten Zeitraum getrennt wird (maximale Leerlaufzeit). Wenn Ihre Internetverbindung wegen Leerlaufs getrennt wurde, kann das Gateway mithilfe der Option **Connect on Demand** (Bei Bedarf verbinden) Ihre Verbindung automatisch wiederherstellen, sobald Sie wieder versuchen, auf das Internet zuzugreifen. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Connect on Demand** (Bei Bedarf verbinden). Geben Sie im Feld *Max Idle Time* (Max. Leerlaufzeit) die Anzahl der Minuten ein, nach deren Ablauf Ihre Internetverbindung getrennt werden soll.
- **Keep Alive: Redial Period** (Verbindung aufrechterhalten: Wahlwiederholung): Wenn Sie diese Option auswählen, überprüft das Gateway regelmäßig Ihre Internetverbindung. Wenn die Verbindung getrennt wird, stellt das Gateway Ihre Verbindung automatisch wieder her. Aktivieren Sie zur Verwendung dieser Option die Optionsschaltfläche **Keep Alive** (Verbindung aufrechterhalten). Legen Sie im Feld *Redial Period* (Wahlwiederholung) fest, wie oft die Internetverbindung vom Gateway überprüft werden soll. Standardmäßig erfolgt die Wahlwiederholung nach **20** Sekunden.

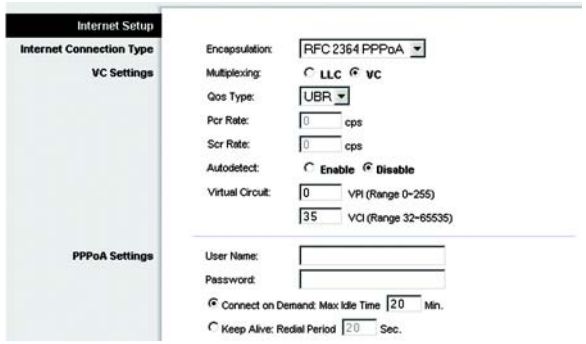



**Abbildung 5-7: RFC 2364 PPPoA**

## Nur Überbrückungsmodus

Wenn Sie das Gateway als Überbrückung verwenden (dadurch agiert das Gateway als Standalone-Modem), wählen Sie die Option **Bridged Mode Only** (Nur Überbrückungsmodus) aus. In diesem Modus sind alle Einstellungen für NAT und Routing deaktiviert.

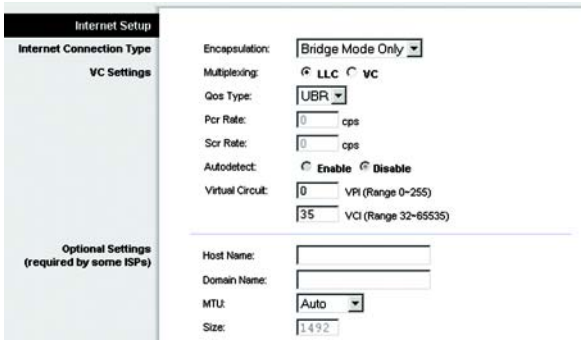



**Abbildung 5-8: Nur Überbrückungsmodus**

## Optionale Einstellungen (für einige ISPs erforderlich)

- **Host Name/Domain Name** (Hostname/Domänenname): In diese Felder können Sie einen Hostnamen bzw. Domänennamen für das Gateway eingeben. Für einige ISPs sind diese Namen zu Identifikationszwecken erforderlich. Erfragen Sie bei Ihrem ISP, ob Ihr Breitband-Internetdienst mit einem Host- und Domänennamen konfiguriert wurde. In den meisten Fällen können diese Felder leer gelassen werden.
- **MTU** und **Size** (MTU und Größe): Mit der MTU-Einstellung (*Maximum Transmission Unit*; Maximale Übertragungseinheit) wird die maximale Paketgröße festgelegt, die zur Netzwerkübertragung zugelassen ist. Wählen Sie **Manual** (Manuell) aus, und geben Sie den gewünschten Wert in das Feld *Size* (Größe) ein. Es wird empfohlen, einen Wert zwischen 1200 und 1500 einzugeben. Die maximale Übertragungseinheit (MTU) wird standardmäßig automatisch festgelegt.

## Netzwerkeinrichtung

- **Router IP** (IP-Adresse des Routers): Die Werte für die lokale IP-Adresse und Subnetzmaske des Gateways sind hier aufgeführt. In den meisten Fällen können die Standardwerte beibehalten werden.
  - **Local IP Address** (Lokale IP-Adresse): Der Standardwert ist **192.168.1.1**.
  - **Subnet Mask** (Subnetzmaske): Der Standardwert ist **255.255.255.0**.
- **Network Address Server Settings (DHCP)** [Einstellungen des Netzwerkadressenservers (DHCP)]: In diesem Bereich können Sie die DHCP-Einstellungen (*Dynamic Host Configuration Protocol* ) des Gateways konfigurieren.
  - **Local DHCP Server** (Lokaler DHCP-Server): Ein DHCP-Server (*Dynamic Host Configuration Protocol*) weist jedem Computer im Netzwerk automatisch eine IP-Adresse zu. Wenn Sie nicht schon über eine IP-Adresse verfügen, ist es äußerst empfehlenswert, das Gateway als DHCP-Server aktiviert zu lassen. Das Gateway kann auch im DHCP-Relay-Modus verwendet werden.
  - **DHCP Relay Server** (DHCP-Relay-Server): Wenn Sie für die Einstellung *Local DHCP Server* (Lokaler DHCP-Server) den DHCP-Relay-Modus aktivieren, geben Sie die IP-Adresse für den DHCP-Server in die entsprechenden Felder ein.
  - **Starting IP Address** (Start-IP-Adresse): Geben Sie einen Wert ein, mit dem der DHCP-Server beim Zuweisen von IP-Adressen beginnen soll. Der Wert muss mindestens 192.168.1.2 betragen, da die Standard-IP-Adresse für das Gateway 192.168.1.1 ist.
  - **Maximum Number of DHCP Users** (Maximale Anzahl der DHCP-Benutzer): Geben Sie die maximale Anzahl von Benutzern bzw. Clients ein, denen eine IP-Adresse zugewiesen werden kann. Diese Zahl hängt von der eingegebenen Start-IP-Adresse ab:
  - **Client Lease Time** (Client-Leasedauer): Bei der Client-Leasedauer handelt es sich um den Zeitraum, in dem ein Computer über seine aktuelle dynamische IP-Adresse eine Verbindung mit dem Gateway herstellen darf. Geben Sie in Minuten an, wie lange diese dynamische IP-Adresse dem Computer zugewiesen bleiben soll.
  - **Static DNS 1-3** (Statisches DNS 1-3): Mit dem DNS (*Domain Name System*) übersetzt das Internet Domänen- oder Website-Namen in Internetadressen oder URLs. Sie erhalten von Ihrem ISP mindestens eine IP-Adresse für den DNS-Server. Hier können Sie bis zu drei IP-Adressen für DNS-Server eingeben. Das Gateway verwendet diese für einen schnelleren Zugriff auf laufende DNS-Server.
  - **WINS**: Mithilfe von WINS (*Windows Internet Naming Service*) werden NetBIOS-Namen in IP-Adressen umgewandelt. Wenn Sie einen WINS-Server verwenden, geben Sie hier die IP-Adresse des Servers ein. Andernfalls lassen Sie dieses Feld leer.
  - **Time Setting** (Zeiteinstellung): Wählen Sie die Zeitzone aus, die sich für den Standort des Gateways eignet. Aktivieren Sie gegebenenfalls das Kontrollkästchen **Automatically adjust clock for daylight saving changes** (Uhr automatisch an Zeitumstellung anpassen).

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

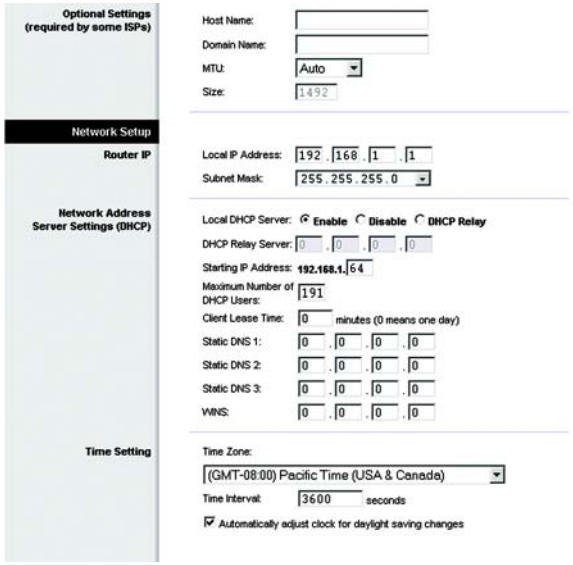



**Abbildung 5-9: Optionale Einstellungen**

## Registerkarte „DDNS“

Das Gateway verfügt über die Funktion **DDNS** (*Dynamic Domain Name System*). Mit DDNS können Sie einer dynamischen Internet-IP-Adresse einen festen Host- und Domänennamen zuweisen. Dies kann sich für das Hosting Ihrer eigenen Website, Ihres FTP-Servers oder anderer Server hinter dem Gateway als nützlich erweisen.

Bevor Sie diese Funktion verwenden können, müssen Sie sich für den DDNS-Dienst unter www.dyndns.org oder www.tzo.com anmelden.

### DDNS

**DDNS Service** (DDNS-Dienst): Wenn der von Ihnen verwendete DDNS-Dienst von DynDNS.org zur Verfügung gestellt wird, wählen Sie aus dem Dropdown-Menü die Option **DynDNS.org** aus. Wenn der von Ihnen verwendete DDNS-Dienst von TZO.com zur Verfügung gestellt wird, wählen Sie aus dem Dropdown-Menü die Option **TZO.com** aus. Wählen Sie zum Deaktivieren des DDNS-Diensts die Option **Disable** (Deaktivieren) aus.

### DynDNS.org

- **User Name** (Benutzername), **Password** (Passwort) und **Host Name** (Hostname): Geben Sie den Benutzernamen, das Passwort und den Hostnamen des mithilfe von DynDNS.org festgelegten Kontos an.
- **Internet IP Address** (Internet-IP-Adresse): Hier ist die aktuelle IP-Adresse des Gateways aufgeführt. Da es sich hierbei um eine dynamische Adresse handelt, kann sie sich ändern.
- **Status**: Hier ist der Status der Verbindung zum DDNS-Dienst aufgeführt.

**Abbildung 5-10: DynDNS.org**

### TZO.com

- **E-mail Address** (E-Mail-Adresse), **Password** (Passwort) und **Domain Name** (Domänenname): Geben Sie die E-Mail-Adresse, das Passwort und den Domänenname des Kontos ein, das Sie bei TZO eingerichtet haben.
- **Internet IP Address** (Internet-IP-Adresse): Hier ist die aktuelle IP-Adresse des Gateways aufgeführt. Da es sich hierbei um eine dynamische Adresse handelt, kann sie sich ändern.
- **Status**: Hier ist der Status der Verbindung zum DDNS-Dienst aufgeführt.

**Abbildung 5-11: TZO.com**

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

## Registerkarte „Advanced Routing“ (Erweitertes Routing)

Über das Fenster *Advanced Routing* (Erweitertes Routing) können Sie die Einstellungen für NAT sowie für das dynamische und statische Routing konfigurieren.

### Erweitertes Routing

- **Operating Mode** (Betriebsmodus): In diesem Bereich können Sie die allgemeinen Routing-Einstellungen des Gateways konfigurieren.
    - **NAT**: Bei NAT handelt es sich um eine Sicherheitsfunktion, die standardmäßig aktiviert ist. Das Gateway kann dank dieser Funktion IP-Adressen Ihres lokalen Netzwerks in eine andere IP-Adresse für die Internetnutzung umwandeln. Um NAT zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disabled** (Deaktiviert).
    - **RIP:** Wenn Sie mehrere Router einsetzen, empfiehlt es sich, das RIP (*Routing Information Protocol*) zu verwenden, damit die Router untereinander Routing-Informationen austauschen können. Aktivieren Sie zur Verwendung von RIP die Optionsschaltfläche **Enabled** (Aktiviert). Behalten Sie andernfalls die Standardeinstellung **Disabled** (Deaktiviert) bei.
    - **Send Default Route** (Standardroute): Wenn Sie die RIP-Version 1 für das Routing verwenden möchten, aktivieren Sie die Optionsschaltfläche **Enabled** (Aktiviert). Behalten Sie andernfalls die Standardeinstellung **Disabled** (Deaktiviert) bei.
    - **Interface** (Schnittstelle): Diese Einstellung ist dann verfügbar, wenn Sie eine statische Route konfiguriert haben und für diese Route eine Schnittstelle auszuwählen ist. Wählen Sie die vom Gateway zu verwendende Schnittstelle aus: **LAN/Wireless** oder **Internet**.
- **Dynamic Routing** (Dynamisches Routing): Mit der Option **Dynamic Routing** (Dynamisches Routing) kann das Gateway automatisch an physische Änderungen in der Netzwerkanordnung angepasst werden. Bei der Verwendung von RIP legt das Gateway die Route der Netzwerkpakete auf der Grundlage der geringsten Anzahl so genannter Hops (Sprüngen) zwischen Quelle und Ziel fest. Das RIP-Protokoll sendet in regelmäßigen Abständen Routing-Information an andere Gateways im Netzwerk.
    - **Transmit RIP Version** (RIP-Version übertragen): Wählen Sie für die Übertragung von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1**, **RIP1-Compatible** (RIP1-kompatibel) oder **RIP2**: Wenn keine RIP-Nachrichten übertragen werden sollen, wählen Sie **None** (Keine) aus.
    - **Receive RIP Version** (RIP-Version empfangen): Wählen Sie für den Empfang von RIP-Nachrichten das gewünschte Protokoll aus: **RIP1** oder **RIP2**: Wenn keine RIP-Nachrichten empfangen werden sollen, wählen Sie **None** (Keine) aus.

**Abbildung 5-12: Erweitertes Routing**

- **Multicast** oder **Broadcast**: RIP kann unter Verwendung beider Methoden gesendet werden. Wenn Sie Multicasting verwenden möchten, wählen Sie **Multicast** aus. Wenn Sie Broadcasting verwenden möchten, wählen Sie **Broadcast** aus.

- **Static Routing** (Statisches Routing): Wenn das Gateway mit mehreren Netzwerken verbunden ist, muss zwischen den Netzwerken u. U. eine statische Route eingerichtet werden. Eine statische Route ist ein vordefinierter Pfad, über den Netzwerkinformationen an einen bestimmten Host oder ein bestimmtes Netzwerk übertragen werden. Ändern Sie die folgenden Einstellungen, um eine statische Route zu erstellen:

  - **Select set number** (Set-Nummer auswählen): Wählen Sie die Anzahl der statischen Routen aus dem Dropdown-Menü aus. Das Gateway unterstützt bis zu 20 Einträge für statische Routen. Wenn Sie eine Route löschen möchten, wählen Sie den entsprechenden Eintrag aus und klicken Sie auf die Schaltfläche **Delete This Entry** (Diesen Eintrag löschen).

  - **Destination IP Address** (Ziel-IP-Adresse): Bei der Ziel-IP-Adresse handelt es sich um die Adresse des entfernten Netzwerks bzw. Hosts, dem Sie eine statische Route zuweisen möchten. Geben Sie die IP-Adresse des Hosts ein, für den Sie eine statische Route erstellen möchten. Wenn Sie eine Route zu einem gesamten Netzwerk erstellen, vergewissern Sie sich, dass für den Netzwerkbereich der IP-Adresse der Wert **0** eingestellt ist.

  - **Subnet Mask** (Subnetzmaske): Geben Sie die Subnetzmaske (auch Netzwerkmaske genannt) ein, mit der festgelegt wird, welcher Bereich einer IP-Adresse der Netzwerkbereich und welcher Bereich der Hostbereich ist.

  - **Gateway**: Geben Sie die IP-Adresse des Gateway-Geräts ein, das eine Verbindung zwischen dem Gateway und dem entfernten Netzwerk bzw. Host ermöglicht.

  - **Hop Count** (Anzahl der Gateways): Gibt die Anzahl der Gateways bis zu den einzelnen Knoten an, bevor das Ziel erreicht wird (max. 16 Gateways). Geben Sie diese Zahl in das entsprechende Feld ein.

- **Show Routing Table** (Routing-Tabelle anzeigen): Klicken Sie auf die Schaltfläche **Show Routing Table** (Routing-Tabelle anzeigen), um ein Fenster zu öffnen, in dem die Art der Datenroutings durch Ihr LAN angezeigt wird. Für jede Route wird die IP-Adresse des Ziel-LANs, die Subnetzmaske, das Gateway und die Schnittstelle angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Daten zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum vorherigen Fenster zurückzukehren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

**Abbildung 5-13: Routing-Tabelle**

# Registerkarte „Wireless“

## Registerkarte „Basic Wireless Settings“ (Grundlegende Wireless-Einstellungen)

Mithilfe dieses Fensters können Sie den Wireless-Netzwerkmodus und die Sicherheit im Wireless-Netzwerkbetrieb festlegen.

### Wireless-Netzwerk

- **Wireless Network Mode** (Wireless-Netzwerkmodus): Wenn sich sowohl 802.11g- als auch 802.11b-Geräte in Ihrem Netzwerk befinden, behalten Sie die Standardeinstellung **Mixed** (Gemischt) bei. Wenn Sie ausschließlich 802.11g-Geräte verwenden, wählen Sie **802.11g** aus. Wenn Sie nur 802.11b-Geräte einsetzen, wählen Sie **802.11b** aus. Wenn Sie den Wireless-Netzwerkbetrieb deaktivieren möchten, wählen Sie **Disabled** (Deaktiviert) aus.

- **Wireless Network Name (SSID)** [Wireless-Netzwerkname (SSID)]: Geben Sie in dieses Feld den Namen für Ihr Wireless-Netzwerk ein. Bei der SSID handelt es sich um den Netzwerknamen, der von allen Geräten im Wireless-Netzwerk verwendet wird. Sie muss für alle Geräte im Wireless-Netzwerk identisch sein. Für die maximal 32 Zeichen lange SSID dürfen alle alphanumerischen Zeichen der Tastatur verwendet werden. Es wird zwischen Groß- und Kleinschreibung unterschieden. Sie sollten die standardmäßige SSID (linksys) in einen eindeutigen Namen Ihrer Wahl ändern.

- **Wireless Channel** (Wireless-Kanal): Wählen Sie aus der Liste den Ihren Netzwerkeinstellungen entsprechenden Kanal aus. Eine korrekte Funktion Ihres Wireless-Netzwerks ist nur gewährleistet, wenn die Übertragung für alle Geräte über denselben Kanal erfolgt. Die Wireless-Computer oder -Clients erkennen den Wireless-Kanal des Gateways automatisch.

- **Wireless SSID Broadcast** (Wireless-SSID-Übertragung): Wenn Wireless-Computer oder -Clients im lokalen Netzwerk nach Wireless-Netzwerken suchen, zu denen sie eine Verbindung herstellen können, erkennen sie die vom Gateway übertragene SSID. Wenn die SSID des Gateways übertragen werden soll, behalten Sie die Standardeinstellung **Enable** (Aktivieren) bei. Wenn die SSID des Gateways nicht übertragen werden soll, wählen Sie **Disable** (Deaktivieren) aus.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

**Abbildung 5-14: Grundlegende Wireless-Einstellungen**

## Registerkarte „Wireless Security“ (Sicherheit im Wireless-Netzwerkbetrieb)

Mit den Wireless-Sicherheitseinstellungen wird die Sicherheit Ihres Wireless-Netzwerks konfiguriert. Das Gateway unterstützt zwei Optionen für die Sicherheit im Wireless-Netzwerkbetrieb: **WPA Pre-Shared Key** (WPA Vorläufiger gemeinsamer Schlüssel) und **WEP** (WPA steht für *Wi-Fi Protected Access*; dies ist ein höherer Sicherheitsstandard als die WEP-Verschlüsselung. WEP ist die Abkürzung für *Wired Equivalent Privacy*.) Im Folgenden erhalten Sie einen Überblick über diese Sicherheitsstandards. Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Gateways erhalten Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb“. Um die Option zur Sicherheit im Wireless-Netzwerkbetrieb zu deaktivieren, wählen Sie im Dropdown-Menü **Security Mode** (Sicherheitsmodus) die Option **Disable** (Deaktivieren) aus.

**Abbildung 5-15: WPA Vorläufiger gemeinsamer Schlüssel**

**WPA Pre-Shared Key** (WPA Vorläufiger gemeinsamer Schlüssel): Geben Sie einen gemeinsamen WPA-Schlüssel mit einer Länge von 8 bis 32 Zeichen ein. Legen Sie anschließend den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Gateway mit, wie oft die Codierschlüssel auszutauschen sind.

**WEP**: WEP ist eine einfache Verschlüsselungsmethode, die nicht so sicher wie WPA ist. Wählen Sie zur Verwendung von WEP einen Wert für **Default Key** (Standardschlüssel; zeigt an, welcher Schlüssel verwendet werden soll) sowie als WEP-Verschlüsselungsebene **64 bits 10 hex digits** (64 Bit 10 Hexadezimalziffern) oder **128 bits 26 hex digits** (128 Bit 26 Hexadezimalziffern) aus. Erstellen Sie anschließend einen WEP-Schlüssel, indem Sie entweder die Passphrase verwenden oder den WEP-Schlüssel manuell eingeben.

- **WEP Encryption** (WEP-Verschlüsselung): WEP ist die Abkürzung für *Wired Equivalent Privacy*. Hierbei handelt es sich um eine Verschlüsselungsmethode zum Schutz der Wireless-Datenkommunikation. WEP basiert auf einem 64-Bit- oder 128-Bit-Schlüssel zur Steuerung des Zugriffs auf Ihr Netzwerk und zur höheren Sicherheit durch Verschlüsselung der Datenübertragung. Um übertragene Daten zu entschlüsseln, müssen alle Geräte im Netzwerk den gleichen WEP-Schlüssel verwenden. Höhere Verschlüsselungsebenen bieten eine höhere Sicherheitsstufe, durch die Komplexität der Verschlüsselung kann jedoch die Netzwerkleistung vermindert werden. Wählen Sie zum Aktivieren von WEP **64 bits 10 hex digits** (64 Bit 10 Hexadezimalziffern) oder **128 bits 26 hex digits** (128 Bit 26 Hexadezimalziffern) aus.
- **Default Transmit Key** (Standard-Übertragungsschlüssel): Legen Sie fest, welcher WEP-Schlüssel (1 bis 4) verwendet werden soll, wenn Daten über das Gateway übertragen werden. Stellen Sie sicher, dass vom Empfangsgerät (Wireless-Computer oder -Client) derselbe Schlüssel verwendet wird.
- **Passphrase**: Sie können anstelle der manuellen Eingabe von WEP-Schlüsseln eine Passphrase eingeben. Mit dieser Passphrase können Sie mindestens einen WEP-Schlüssel erstellen. Hierbei wird zwischen Groß- und Kleinschreibung unterschieden, und die Länge von 32 alphanumerischen Zeichen darf nicht überschritten werden. (Diese Passphrase ist nur mit Wireless-Produkten von Linksys kompatibel und kann nicht mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung verwendet werden. Wenn Sie mit Wireless-Produkten anderer Hersteller oder mit dem Windows XP-Dienstprogramm zur konfigurationsfreien Verbindung kommunizieren möchten, notieren Sie sich den im Feld *Key 1* (Schlüssel 1) generierten WEP-Schlüssel und geben Sie ihn manuell in den Wireless-Computer oder -Client ein.) Klicken Sie nach Eingabe der Passphrase auf **Generate** (Generieren), um WEP-Schlüssel zu erstellen.
- **WEP Keys 1-4** (WEP-Schlüssel 1 - 4): Mithilfe von WEP-Schlüsseln können Sie ein Verschlüsselungsschema für Übertragungen im Wireless-Netzwerk erstellen. Wenn Sie keine Passphrase verwenden, geben Sie manuell einen Wertesatz ein. (Lassen Sie keine Schlüsselfelder leer, und geben Sie nicht in alle Schlüsselfelder den Wert **0** ein, da es sich hierbei nicht um gültige Schlüsselwerte handelt.) Wenn Sie die 64-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 10 hexadezimale Zeichen betragen. Wenn Sie die 128-Bit-WEP-Verschlüsselung verwenden, muss die Schlüssellänge genau 26 hexadezimale Zeichen betragen. Gültige hexadezimale Zeichen sind Zahlen von 0 bis 9 und Buchstaben von A bis F.

**Abbildung 5-16: WEP**

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen). Genauere Anweisungen zur Konfiguration der Sicherheit im Wireless-Netzwerkbetrieb des Gateways erhalten Sie in „Anhang B: Sicherheit im Wireless-Netzwerkbetrieb“.

## Registerkarte „Wireless Access“ (Wireless-Zugriff)

### Wireless-Netzwerkzugriff

**Wireless Network Access** (Wireless-Netzwerkzugriff): Wählen Sie **Allow All** (Alle zulassen) aus, wenn allen Computern der Zugriff auf das Wireless-Netzwerk ermöglicht werden soll. Soll der Zugriff eingeschränkt werden, wählen Sie **Restrict Access** (Zugriff beschränken) und anschließend zum Verweigern des Zugriffs für bestimmte Computer **Prevent** (Verweigern) oder zum Gestatten des Zugriffs für bestimmte Computer **Permit only** (Nur Zugriff) aus. Klicken Sie auf die Schaltfläche **Edit MAC Address Access List** (MAC-Adressen-Filterliste bearbeiten). Daraufhin wird das Fenster *Mac Address Filter List* (MAC-Adressen-Filterliste) angezeigt.

Geben Sie die MAC-Adressen der Computer ein, die Sie festlegen möchten. Wenn Sie eine Liste der MAC-Adressen für Wireless-Computer oder -Clients anzeigen möchten, klicken Sie auf die Schaltfläche **Wireless Client MAC List** (MAC-Liste der Wireless-Clients).

Im Fenster *Wireless Client MAC List* (MAC-Liste der Wireless-Clients) werden Computer mit ihrer jeweiligen IP- und MAC-Adresse aufgeführt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), damit die aktuellsten Informationen angezeigt werden. Wenn der MAC-Adressen-Filterliste ein bestimmter Computer hinzugefügt werden soll, aktivieren Sie das Kontrollkästchen **Enable MAC Filter** (MAC-Filter aktivieren) und klicken Sie anschließend auf die Schaltfläche **Update Filter List** (Filterliste aktualisieren). Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Wireless Client MAC List* (MAC-Liste der Wireless-Clients) zurückzukehren.

Klicken Sie im Fenster *Wireless Client MAC List* (MAC-Liste der Wireless-Clients) zum Speichern der Liste auf die Schaltfläche **Save Settings** (Einstellungen speichern) oder auf **Cancel Changes** (Änderungen verwerfen), um Ihre Einträge zu löschen.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

**Abbildung 5-17: Wireless-Netzwerkzugriff**

**Abbildung 5-18: MAC-Adressen-Filterliste**

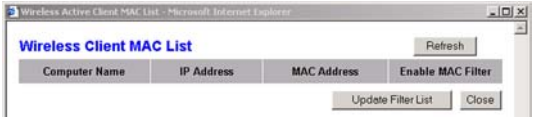



**Abbildung 5-19: MAC-Liste der Wireless-Clients**

## Registerkarte „Advanced Wireless Settings“ (Erweiterte Wireless-Einstellungen)

### Erweitertes Wireless

In diesem Fenster können Sie auf die folgenden erweiterten Wireless-Funktionen zugreifen: Authentifizierungstyp, Gesteuerte Übertragungsrate, Beacon-Intervall, DTIM-Intervall, Fragmentierungsschwelle und RTS-Schwelle.

- **Authentication Type** (Authentifizierungstyp): Standardmäßig ist die Option **Auto** (Automatisch) ausgewählt, mit der sowohl der Authentifizierungstyp **Open System** (Offenes System) als auch **Shared Key** (Freigegebener Schlüssel) verwendet werden kann. Beim Authentifizierungstyp **Open System** (Offenes System) verwenden Absender und Empfänger zur Authentifizierung keinen WEP-Schlüssel, sie können WEP jedoch zur Datenverschlüsselung verwenden. Wenn nur die Open System-Authentifizierung zugelassen werden soll, wählen Sie **Open System** (Offenes System) aus. Beim Authentifizierungstyp **Shared Key** (Freigegebener Schlüssel) verwenden Absender und Empfänger sowohl zur Authentifizierung als auch zur Datenverschlüsselung einen WEP-Schlüssel. Soll nur die Shared Key-Authentifizierung zugelassen werden, wählen Sie **Shared Key** (Freigegebener Schlüssel) aus. Es wird empfohlen, diese Option im Standardmodus **Auto** (Automatisch) zu belassen, da einige Clients nicht für die Option **Shared Key** (Freigegebener Schlüssel) konfiguriert werden können.
- **Control Tx Rates** (Gesteuerte Übertragungsraten): Die Standardübertragungsrate ist auf **Auto** (Automatisch) eingestellt. Diese Rate sollte gemäß der Geschwindigkeit Ihres Wireless-Netzwerks eingestellt werden. Wählen Sie eine der Übertragungsgeschwindigkeiten aus, oder behalten Sie die standardmäßig eingestellte Option **Auto** (Automatisch) bei, wodurch das Gateway automatisch die schnellstmögliche Datenrate verwendet und die Funktion **Auto-Fallback** (Automatisches Fallback) aktiviert wird. Mit der Funktion für automatisches Fallback wird die optimale Verbindungsgeschwindigkeit zwischen dem Gateway und einem Wireless-Client ermittelt.
- **Beacon Interval** (Beacon-Intervall): Der Standardwert ist **100**. Der Wert des Beacon-Intervalls gibt das Sendeintervall des Beacons an. Ein Beacon ist eine Paket, das vom Gateway zur Synchronisierung des Wireless-Netzwerks übertragen wird.
- **DTIM Interval** (DTIM-Intervall): Der Standardwert ist **1**. Mit diesem Wert wird der DTIM-Intervall (*Delivery Traffic Indication Message*) angegeben. Ein DTIM-Feld ist ein Zeitkontrollfeld, das Clients über das nächste Fenster informiert, in dem nach Broadcast- und Multicast-Meldungen gesucht wird. Wenn das Gateway Broadcast- oder Multicast-Meldungen für die zugewiesenen Clients gepuffert hat, sendet es die nächste DTIM mit einem DTIM-Intervallwert. Die zugewiesenen Clients empfangen das Beacon-Signal und sind zum Empfang der Broadcast- und Multicast-Meldungen bereit.
- **Fragmentation Threshold** (Fragmentierungsschwelle): Dieser Wert sollte bei dem Standardwert von **2346** belassen werden. Er gibt die maximale Größe eines Pakets an, bevor die Daten in mehrere Pakete unterteilt werden. Wenn Sie eine hohe Paketfehlerrate wahrnehmen, können Sie die Fragmentierungsschwelle leicht anheben. Wenn die Fragmentierungsschwelle zu niedrig liegt, kann dies zu einer Verringerung der Netzwerkleistung führen. Es wird nur eine geringfügige Änderung dieses Werts empfohlen.
- **RTS Threshold** (RTS-Schwelle): Dieser Wert sollte bei dem Standardwert von **2347** belassen werden. Bei einem schwankenden Datenfluss wird eine nur geringfügige Änderung empfohlen. Wenn ein Netzwerkpaket kleiner als die voreingestellte RTS-Schwellengröße ist, wird der RTS/CTS-Mechanismus nicht aktiviert. Das Gateway sendet RTS-Blöcke (*Request to Send*) an eine bestimmte Empfangsstation und handelt das Senden eines Datenblocks aus. Nach dem Empfang eines RTS-Blocks antwortet die Wireless-Station mit einem CTS-Block (*Clear to Send*), um das Recht, mit der Übertragung zu beginnen, zu bestätigen.

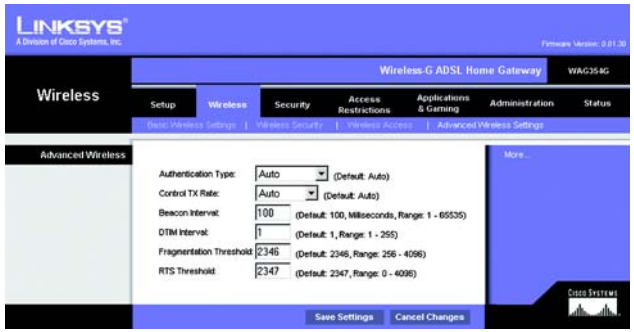



**Abbildung 5-20: Erweiterte Wireless-Einstellungen**

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

## Registerkarte „Security“ (Sicherheit)

In diesem Fenster werden die Einstellungen für VPN-Passthrough, Firewall und Filter angezeigt. Verwenden Sie diese Funktionen, um die Sicherheit des Netzwerks zu erhöhen.

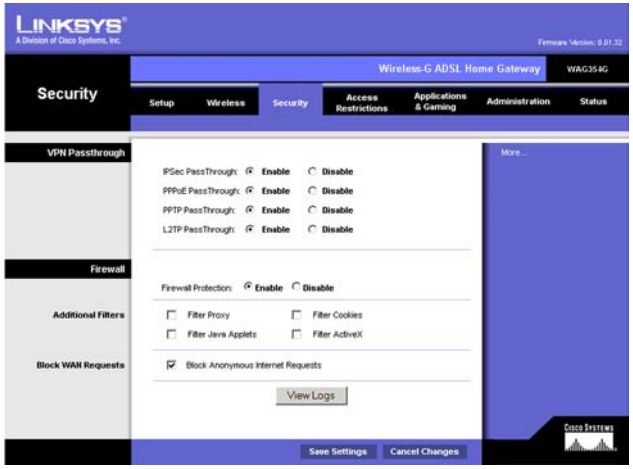



**Abbildung 5-21: Sicherheit**

### VPN-Passthrough

VPN (*Virtual Private Networking*) ist eine Sicherheitsmaßnahme, mit der eine sichere Verbindung zwischen zwei entfernten Standorten hergestellt wird. Konfigurieren Sie die folgenden Einstellungen so, dass das Gateway die Übertragung durch VPN-Tunnel zulässt.

- **IPSec Passthrough** (IPSec-Passthrough): IPSec (*Internet Protocol Security*) ist ein Protokollsatz, der zum sicheren Paketaustausch auf der IP-Ebene verwendet wird. Um IPSec-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren). Um IPSec-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disable** (Deaktivieren).
- **PPPoE Passthrough** (PPPoE-Passthrough): Mit PPPoE-Passthrough können Sie die von Ihrem ISP bereitgestellte PPPoE-Client-Software auf Ihren PCs verwenden. Einige ISPs verlangen, dass diese Funktion für das Gateway verwendet wird. Um PPPoE-Passthrough zu aktivieren, klicken Sie auf die Schaltfläche **Enable** (Aktivieren). Um PPPoE-Passthrough zu deaktivieren, klicken Sie auf die Schaltfläche **Disable** (Deaktivieren).
- **PPTP Passthrough** (PPTP-Passthrough): PPTP-Passthrough (*Point-to-Point Tunneling Protocol Passthrough*) ist eine Methode zur Aktivierung von VPN-Sitzungen auf Windows NT 4.0- oder Windows 2000-Servern. Um PPTP-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren). Um PPTP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disable** (Deaktivieren).
- **L2TP Passthrough** (L2TP-Passthrough): Bei L2TP-Passthrough (*Layering 2 Tunneling Protocol Passthrough*) handelt es sich um eine Erweiterung von PPTP (*Point-to-Point Tunneling Protocol*), mit der VPNs über das Internet betrieben werden können. Um P2TP-Passthrough zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren). Um P2TP-Passthrough zu deaktivieren, klicken Sie auf die Optionsschaltfläche **Disable** (Deaktivieren).

### Firewall

Sie können die Firewall aktivieren oder deaktivieren, Filter zum Blockieren bestimmter Internetdatentypen auswählen und anonyme Internet-Anfragen blockieren.

Klicken Sie zum Verwenden der Firewall auf **Enable** (Aktivieren). Wenn die Firewall nicht verwendet werden soll, klicken Sie auf **Disable** (Deaktivieren).

## Zusätzliche Filter

- **Filter Proxy** (Filterproxy): Die Verwendung von WAN-Proxyservern kann die Sicherheit des Gateways beeinträchtigen. Wenn Sie den Filterproxy ablehnen, wird der Zugriff auf alle WAN-Proxyserver deaktiviert. Aktivieren Sie zum Verwenden der Proxy-Filterung das entsprechende Kontrollkästchen.
- **Filter Cookies** (Cookies filtern): Bei einem Cookie handelt es sich um Daten, die auf Ihrem Computer gespeichert sind und von Websites beim Zugriff auf diese Sites verwendet werden. Aktivieren Sie zum Verwenden der Cookie-Filterung das entsprechende Kontrollkästchen.
- **Filter Java Applets** (Java-Applets filtern): Bei Java handelt es sich um eine Programmiersprache für Websites. Wenn Sie Java-Applets ablehnen, können Sie u. U. nicht auf Websites zugreifen, die mit dieser Programmiersprache erstellt wurden. Aktivieren Sie zum Verwenden der Java Applet-Filterung das entsprechende Kontrollkästchen.
- **Filter ActiveX** (ActiveX filtern): Bei ActiveX handelt es sich um eine Programmiersprache für Websites. Wenn Sie ActiveX ablehnen, können Sie u. U. nicht auf Websites zugreifen, die mit dieser Programmiersprache erstellt wurden. Aktivieren Sie zum Verwenden der ActiveX-Filterung das entsprechende Kontrollkästchen.

## WAN-Anfragen blockieren

- **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren): Mit dieser Option können Sie Ihr Netzwerk vor Ping-Angriffen oder dem Erkennen durch andere Internetbenutzer schützen. Darüber hinaus können Sie mit dieser Option die Sicherheit Ihres Netzwerks erhöhen, indem Ihre Netzwerk-Ports nicht angezeigt werden und Ihr Netzwerk vor Angreifern aus dem Internet besser geschützt ist. Aktivieren Sie die Option **Block Anonymous Internet Requests** (Anonyme Internet-Anfragen blockieren), um anonyme Internet-Anfragen zu blockieren bzw. deaktivieren Sie die Option, um anonyme Internet-Anfragen zuzulassen.

Wenn die Aktivitätsprotokolle für die Sicherheitsmaßnahmen angezeigt werden sollen, klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen). Klicken Sie auf die Schaltfläche **Clear** (Löschen), um die Protokollinformationen zu löschen. Klicken Sie auf die Schaltfläche **pageRefresh** (Seite aktualisieren), um die Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Previous Page** (Vorherige Seite), um zur vorherigen Informationsseite zu wechseln. Klicken Sie auf die Schaltfläche **Next Page** (Nächste Seite), um zur nächsten Informationsseite zu wechseln.

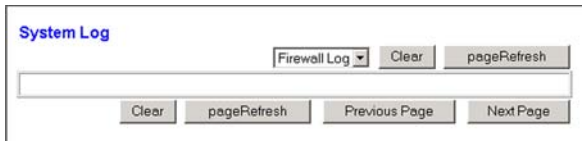



**Abbildung 5-22: Firewall-Protokoll**

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

# Registerkarte „Access Restrictions“ (Zugriffsbeschränkungen)

## Registerkarte „Internet Access“ (Internetzugriff)

Im Fenster *Internet Access* (Internetzugriff) können Sie bestimmte Arten der Internetverwendung blockieren bzw. zulassen. Sie können für bestimmte Computer Richtlinien für den Internetzugriff einrichten und Websites nach URL-Adresse oder Schlüsselwort blockieren.

**Internet Access Policy** (Richtlinien für Internetzugriff): Der Zugriff kann mithilfe von Richtlinien verwaltet werden. Mit den Einstellungen in diesem Fenster können Sie Zugriffsrichtlinien erstellen, nachdem Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern) geklickt haben. Wenn Sie aus dem Dropdown-Menü eine Richtlinie ausgewählt haben, werden die Einstellungen dieser Richtlinie angezeigt. Um eine Richtlinie zu löschen, wählen Sie die Nummer dieser Richtlinie aus und klicken Sie auf die Schaltfläche **Delete** (Löschen). Um alle Richtlinien anzuzeigen, klicken Sie auf die Schaltfläche **Summary** (Zusammenfassung). (Sie können Richtlinien aus dem Fenster *Summary* (Zusammenfassung) löschen, indem Sie die entsprechende Richtlinie auswählen und auf die Schaltfläche **Delete** (Löschen) klicken. Um zum Fenster **Internet Access** (Internetzugriff) zurückzukehren, klicken Sie auf die Schaltfläche **Close** (Schließen).)

**Status**: Die Richtlinien sind standardmäßig deaktiviert. Um eine Richtlinie zu aktivieren, wählen Sie im Dropdown-Menü die Richtlinien-Nummer aus, und aktivieren Sie die Optionsschaltfläche *Enable* (Aktivieren).

So erstellen Sie eine Richtlinie für den Internetzugriff:

1. Wählen Sie im Dropdown-Menü *Internet Access Policy* (Richtlinien für Internetzugriff) eine Nummer aus.
2. Um diese Richtlinie zu aktivieren, klicken Sie auf die Optionsschaltfläche **Enable** (Aktivieren).
3. Geben Sie im Feld **Policy Name** (Richtlinienname) einen Namen für die Richtlinie ein.

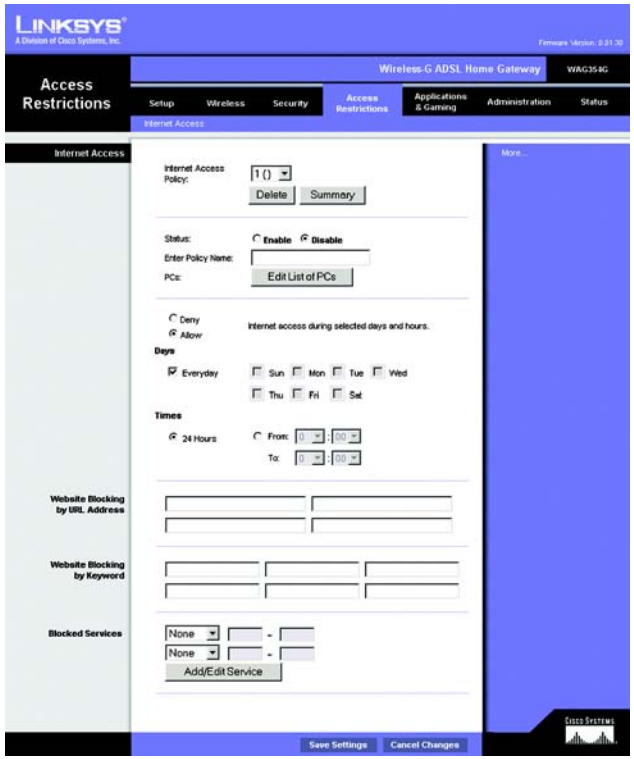



**Abbildung 5-23: Internetzugriff**

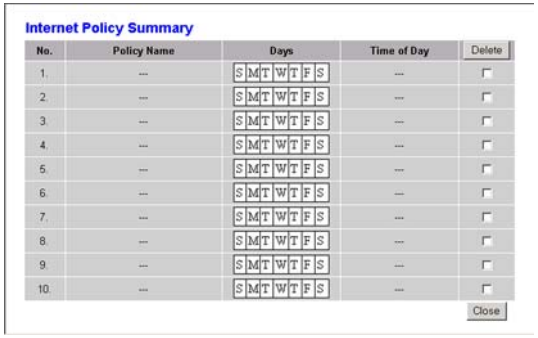



**Abbildung 5-24: Internet-Richtlinien - Zusammenfassung**

4. Klicken Sie auf die Schaltfläche **Edit List of PCs** (Liste der PCs bearbeiten), um die PCs auszuwählen, für die die Richtlinie gelten soll. Das Fenster *List of PCs* (PC-Liste) wird angezeigt. Sie können einen PC nach MAC-Adresse oder IP-Adresse auswählen. Sie können auch mehrere IP-Adressen eingeben, wenn diese Richtlinie für eine Gruppe von PCs gelten soll. Nachdem Sie Ihre Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um Ihre Änderungen anzuwenden, oder auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.
5. Klicken Sie auf die entsprechende Option **Deny** (Verweigern) oder **Allow** (Zulassen), je nachdem, ob Sie den Internetzugriff für die PCs, die Sie im Fenster *List of PCs* (PC-Liste) aufgeführt haben, blockieren oder zulassen möchten.
6. Bestimmen Sie, an welchen Tagen und zu welcher Uhrzeit diese Richtlinie jeweils in Kraft treten soll. Wählen Sie die einzelnen Tage aus, an denen die Richtlinie in Kraft treten soll, oder wählen Sie die Option **Everyday** (Jeden Tag) aus. Geben Sie anschließend die Stunden und Minuten ein, um den Zeitraum festzulegen, in dem die Richtlinie in Kraft treten soll, oder wählen Sie die Option **24 Hours** (24 Stunden) aus.
7. Wenn Sie Websites mit bestimmten URL-Adressen blockieren möchten, geben Sie die entsprechenden URLs in jeweils ein separates Feld neben *Website Blocking by URL Address* (Website nach URL-Adresse blockieren) ein.
8. Wenn Sie Websites mithilfe bestimmter Schlüsselwörter blockieren möchten, geben Sie die entsprechenden Schlüsselwörter in jeweils ein separates Feld neben *Website Blocking by Keyword* (Website nach Schlüsselwort blockieren) ein.
9. Sie können den Zugang zu verschiedenen Diensten filtern, auf die über das Internet, z. B. FTP oder Telnet, zugegriffen werden kann, indem Sie diese Dienste in den Dropdown-Menüs neben *Blocked Services* (Blockierte Dienste) auswählen.

   Geben Sie anschließend den Bereich der Ports ein, den Sie filtern möchten.

   Wenn der Dienst, den Sie blockieren möchten, nicht in der Liste aufgeführt ist, oder wenn Sie die Einstellungen eines Diensts bearbeiten möchten, klicken Sie auf die Schaltfläche **Add/Edit Service** (Dienst hinzufügen/bearbeiten). Daraufhin wird das Fenster *Port Services* (Anschlussdienste) angezeigt.

   Um einen Dienst hinzuzufügen, geben Sie den Namen des Diensts in das Feld *Service Name* (Dienstname) ein. Wählen Sie im Dropdown-Menü *Protocol* (Protokoll) das entsprechende Protokoll aus, und geben Sie den dessen Bereich in die Felder *Port Range* (Anschlussbereich) ein. Klicken Sie anschließend auf die Schaltfläche **Add** (Hinzufügen).

   Um einen Dienst zu bearbeiten, wählen Sie diesen aus der Liste auf der rechten Seite aus. Ändern Sie den Namen, die Protokolleinstellung oder den Anschlussbereich. Klicken Sie anschließend auf die Schaltfläche **Modify** (Bearbeiten).

   Um einen Dienst zu löschen, wählen Sie diesen aus der Liste auf der rechten Seite aus. Klicken Sie anschließend auf die Schaltfläche **Delete** (Löschen).

   Wenn Sie die gewünschten Änderungen im Fenster *Port Services* (Anschlussdienste) vorgenommen haben, klicken Sie auf die Schaltfläche **Apply** (Anwenden), um die Änderungen zu speichern. Wenn Sie Ihre Änderungen verwerfen möchten, klicken Sie auf die Schaltfläche **Cancel** (Abbrechen). Um das Fenster *Port Services* (Anschlussdienste) zu schließen und zum Fenster *Access Restrictions* (Zugriffsbeschränkungen) zurückzukehren, klicken Sie auf die Schaltfläche **Close** (Schließen).
10. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um die Einstellungen der Richtlinie zu speichern. Um die Einstellungen der Richtlinie rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

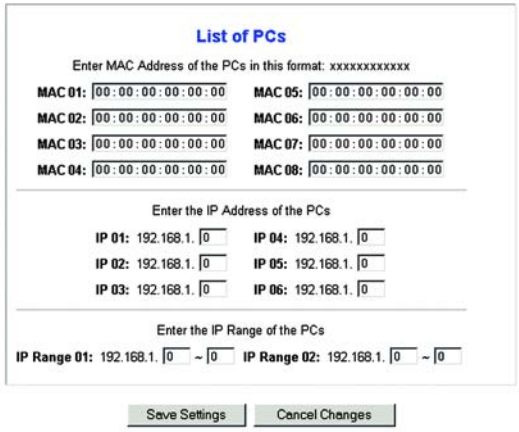



**Abbildung 5-25: PC-Liste**

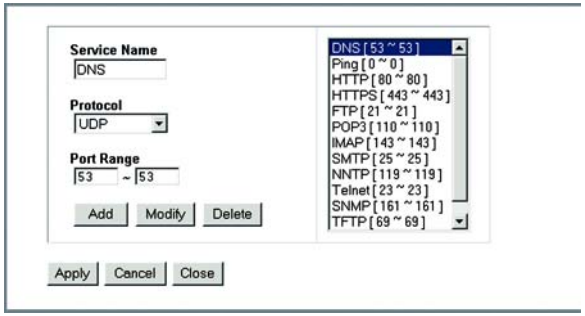



**Abbildung 5-26: Dienst hinzufügen/bearbeiten**

# Registerkarte „Applications and Gaming“ (Anwendungen und Spiele)

## Registerkarte „Single Port Forwarding“ (Einfaches Port-Forwarding)

### Einfaches Port-Forwarding

Verwenden Sie das Fenster *Single Port Forwarding* (Einfaches Port-Forwarding), wenn ein bestimmter Port geöffnet werden soll, damit Benutzer im Internet die Server hinter dem Gateway erkennen können (zu diesen Servern können FTP- oder E-Mail-Server zählen). Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden PC weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein. Darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

- **Port Map List** (Liste der Port-Zuweisung): In diesem Bereich passen Sie den Port-Dienst an Ihre Anwendungen an.
  - **Application** (Anwendung): Geben Sie den Namen der Anwendung in das entsprechende Feld ein.
  - **External Port** (Externer Port) und **Internal Port** (Interner Port): Geben Sie die Nummern für den externen und internen Port ein.
  - Protocol (Protokoll): Wählen Sie das Protokoll aus, das Sie für die jeweilige Anwendung verwenden möchten: **TCP** oder **UDP**.
  - **IP Address** (IP-Adresse): Geben Sie die IP-Adresse des entsprechenden Computers ein.
  - **Enabled** (Aktiviert): Klicken Sie auf **Enabled** (Aktiviert), um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

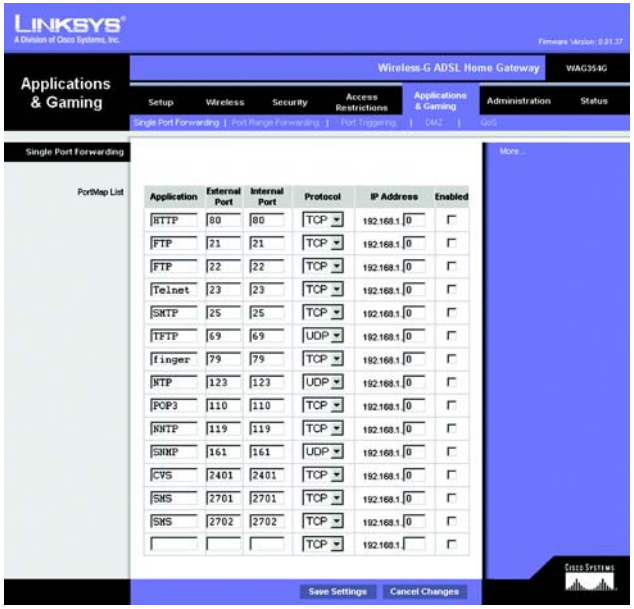



**Abbildung 5-27: Einfaches Port-Forwarding**

## Registerkarte „Port Range Forwarding“ (Weiterleitung an einen Anschlussbereich)

Im Fenster *Port Range Forwarding* (Weiterleitung an einen Anschlussbereich) können Sie öffentliche Dienste auf dem Netzwerk festlegen (z. B. Web-, FTP-, E-Mail-Server oder andere spezielle Internetanwendungen). (Unter speziellen Internetanwendungen versteht man alle Anwendungen, die über den Internetzugang Funktionen wie z. B. Videokonferenzen oder Internet-Spiele ausführen. Bei einigen Internetanwendungen ist keine Weiterleitung erforderlich.)

Wenn Anfragen dieser Art von Benutzern über das Internet an Ihr Netzwerk gesendet werden, leitet das Gateway diese Anfragen an den entsprechenden PC weiter. Auf jedem Computer, dessen Anschluss weitergeleitet wird, muss die DCHP-Client-Funktion deaktiviert sein. Darüber hinaus sollte jedem Computer eine neue statische IP-Adresse zugewiesen werden, da die IP-Adresse bei Verwendung der DHCP-Funktion u. U. geändert wird.

- **Application** (Anwendung): Geben Sie den Namen der Anwendung in das entsprechende Feld ein.
- **Start** (Von) und **End** (Bis): Geben Sie die Anfangs- und Endnummern des Anschlussbereichs ein, der weitergeleitet werden soll.
- **Protocol** (Protokoll): Wählen Sie das Protokoll aus, das Sie für die jeweilige Anwendung verwenden möchten: **TCP**, **UDP** oder **Both** (Beide).
- **IP Address** (IP-Adresse): Geben Sie die IP-Adresse des entsprechenden Computers ein.
- **Enable** (Aktivieren): Aktivieren Sie das Kontrollkästchen **Enable** (Aktivieren), um die Weiterleitung für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

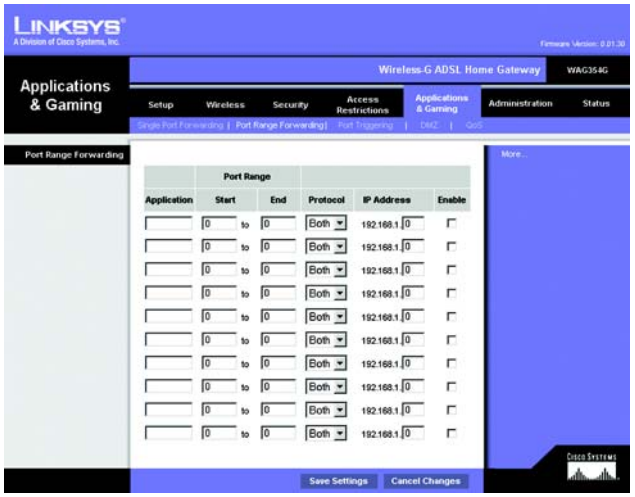



**Abbildung 5-28: Port Range Forwarding (Weiterleitung an einen Anschlussbereich)**

## Registerkarte „Port Triggering“

Port-Triggering wird bei speziellen Anwendungen verwendet, über die ein Anschluss auf Anfrage geöffnet werden kann. Bei dieser Funktion überprüft das Gateway ausgehende Daten auf spezielle Anschlussnummern. Das Gateway speichert die IP-Adresse des Computers, der Daten zur Übertragung abruft. Wenn die abgerufenen Daten über das Gateway übertragen werden, werden die Daten über IP-Adresse und Port-Mapping-Regeln an den entsprechenden Computer weitergeleitet.

- **Application** (Anwendung): Geben Sie für jede Anwendung den gewünschten Namen ein.
- **Triggering Range** (Triggering-Bereich): Geben Sie die Anfangs- und Endnummern der Ports für den Triggering-Bereich ein.
- **Forwarded Range** (Weiterleitungsbereich): Geben Sie die Anfangs- und Endnummern der Ports für den Weiterleitungsbereich ein.
- **Enable** (Aktivieren): Aktivieren Sie das Kontrollkästchen **Enable** (Aktivieren), um das Port-Triggering für die ausgewählte Anwendung zu aktivieren.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

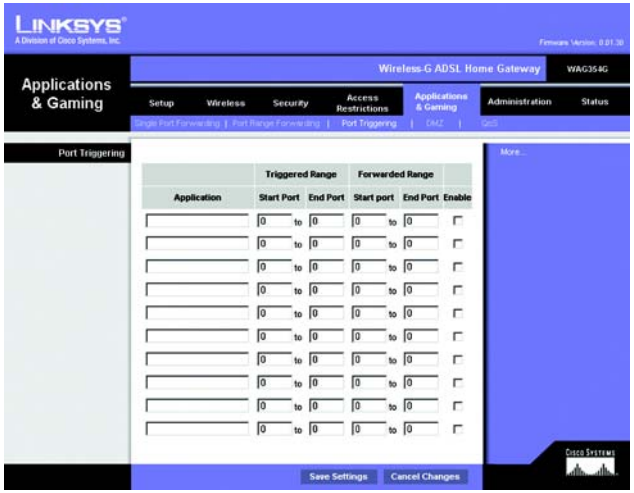



**Abbildung 5-29: Port-Triggering**

## Registerkarte „DMZ“

Über das Fenster *DMZ* kann mithilfe von DMZ-Hosting für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser spezielle Dienste (z. B. Internet-Spiele und Videokonferenzen) nutzen kann. Mit DMZ-Hosting werden alle Ports für einen Computer gleichzeitig weitergeleitet, im Unterschied zu **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich), bei dem nur maximal 10 Anschlussbereiche weitergeleitet werden können.

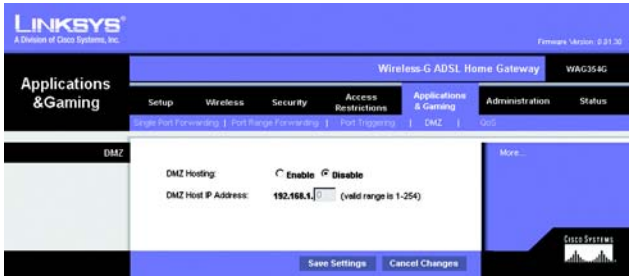



**Abbildung 5-30: DMZ**

- **DMZ Hosting** (DMZ-Hosting): Mit der DMZ-Funktion (*Demilitarized Zone*; Entmilitarisierte Zone) kann für einen lokalen Benutzer eine Verbindung zum Internet hergestellt werden, damit dieser einen speziellen Dienst, wie z. B. Internet-Spiele oder Videokonferenzen, nutzen kann. Klicken Sie auf **Enable** (Aktivieren), um diese Funktion zu verwenden. Klicken Sie auf **Disable** (Deaktivieren), um die DMZ-Funktion zu deaktivieren.

- **DMZ Host IP Address** (IP-Adresse des DMZ-Hosts): Um einen Computer mit dem Internet zu verbinden, geben Sie die IP-Adresse des Computers ein. Weitere Informationen zum Ermitteln einer IP-Adresse eines Computers finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

## Registerkarte „QoS“

### QoS

QoS (*Quality of Service*) sorgt bei Netzwerkverkehr mit hoher Priorität, beispielsweise bei anspruchsvollen Echtzeitanwendungen wie Internettelefonie oder Videokonferenzen, für besseren Service.

**Enable/Disable** (Aktivieren/Deaktivieren): Wählen Sie zum Verwenden von QoS die Option **Enable** (Aktivieren) aus. Behalten Sie andernfalls die Standardeinstellung **Disable** (Deaktivieren) bei.

### Anwendungsbasierte QoS

Über **Application-based QoS** (Anwendungsbasierte QoS) werden Informationen beim Übertragen und Empfangen verwaltet. Je nachdem, welche Einstellungen im Fenster *QoS* festgelegt sind, weist diese Funktion den Informationen von fünf voreingestellten Anwendungen sowie drei zusätzlich angegebenen Anwendungen eine hohe oder niedrige Priorität zu.

**High priority/Medium priority/Low priority** (Hohe Priorität/Mittlere Priorität/Niedrige Priorität): Wählen Sie für jede der Anwendungen **High priority** (Hohe Priorität; Datenverkehr in dieser Warteschlange belegt 60 % der gesamten Bandbreite), **Medium priority** (Mittlere Priorität; Datenverkehr in dieser Warteschlange belegt 18 % der gesamten Bandbreite) oder **Low priority** (Niedrige Priorität; Datenverkehr in dieser Warteschlange belegt 1 % der gesamten Bandbreite).

**FTP** (*File Transfer Protocol*): Ein Protokoll für die Übertragung von Dateien über ein TCP/IP-Netzwerk (Internet, UNIX usw.). Nachdem HTML-Seiten für eine Website auf einem lokalen System gestaltet wurden, werden sie üblicherweise über FTP auf den Server geladen.

**HTTP** (*HyperText Transport Protocol*): Kommunikationsprotokoll, das zum Anschließen von Servern an das World Wide Web verwendet wird. Seine Hauptfunktion besteht darin, eine Verbindung mit einem Webserver herzustellen und HTML-Seiten an den Web-Browser des Clients zu übertragen.

**Telnet**: Ein Protokoll zur Terminal-Emulation, das häufig in Internet- und TCP/IP-basierten Netzwerken verwendet wird. Dadurch wird Benutzern an Terminals oder Computern ermöglicht, sich bei entfernten Geräten anzumelden und Programme auszuführen.

**SMTP** (*Simple Mail Transfer Protocol*): **Das standardmäßige E-Mail-Protokoll im Internet.** Ein TCP/IP-Protokoll, mit dem das Meldungsformat sowie der MTA (*Message Transfer Agent*; Meldungsübertragungsagent) festgelegt werden, der die Mail speichert und weiterleitet.

**POP3** (*Post Office Protocol 3*): Ein im Internet verbreitet eingesetzter Standard-Mailserver. Er bietet einen Meldungsspeicher, in dem eingehende Mails gespeichert werden, bis sich der entsprechende Empfänger anmeldet und die Mails herunterlädt. POP3 ist ein einfaches System mit wenig Auswahlmöglichkeiten. Alle ausstehenden Meldungen und Anhänge werden zur selben Zeit heruntergeladen. POP3 verwendet das SMTP-Meldungsprotokoll.

**Specific Port#** (Spezielle Anschlussnummer): Sie können drei weitere Anwendungen hinzufügen, indem Sie deren jeweilige Anschlussnummern in diese Felder eingeben.

Klicken Sie nach dem Vornehmen aller Änderungen in diesem Fenster auf die Schaltfläche **Save Settings** (Einstellungen speichern), oder klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen), um die Änderungen rückgängig zu machen.

**Abbildung 5-31: QoS**

# Registerkarte „Administration“ (Verwaltung)

## Registerkarte „Management“ (Verwaltungsfunktionen)

Über das Fenster *Management* (Verwaltungsfunktionen) können Sie die Einstellungen für den Gateway-Zugriff ändern sowie die Verwaltungsfunktionen für SNMP (*Simple Network Management Protocol*), UPnP (*Universal Plug and Play*), IGMP-Proxy (*Internet Group Multicast Protocol*) und WLAN konfigurieren.

### Gateway Access (Gateway-Zugriff)

**Local Gateway Access** (Lokaler Gateway-Zugriff): Um die Sicherheit des Gateways zu gewährleisten, werden Sie beim Zugriff auf das webbasierte Dienstprogramm des Gateways zur Eingabe Ihres Passworts aufgefordert. Der Standardbenutzername und das Standardpasswort sind **admin**.

- **Gateway Userlist** (Gateway-Benutzerliste): Wählen Sie die Nummer des Benutzers aus dem Dropdown-Menü aus.
- **Gateway Username** (Gateway-Benutzername): Geben Sie den Standardbenutzernamen **admin** ein. Es wird empfohlen, dass Sie Ihren Standardbenutzernamen in einen persönlichen Benutzernamen ändern.
- **Gateway Password** (Gateway-Passwort): Wir empfehlen, das Standardpasswort **admin** in ein Passwort Ihrer Wahl zu ändern.
- **Re-enter to confirm** (Zur Bestätigung erneut eingeben): Geben Sie das neue Gateway-Passwort erneut ein, um es zu bestätigen.

**Remote Gatway Access** (Entfernter Gateway-Zugriff): Mit dieser Funktion können Sie von einem entfernten Standort aus über das Internet auf das Gateway zugreifen.

- **Remote Management** (Remote-Management): Mit dieser Funktion können Sie das Gateway von einem entfernten Standort aus über das Internet verwalten. Klicken Sie zum Aktivieren von **Remote Management** (Remote-Management) auf **Enable** (Aktivieren).

  **WICHTIG:** Durch Aktivieren der Option **Remote Management** (Remote-Management) kann jeder Benutzer, der Ihr Passwort kennt, von jedem beliebigen Standort im Internet das Gateway konfigurieren.

- **Management Port** (Management-Port): Geben Sie die Anschlussnummer ein, die Sie für den entfernten Zugriff auf das Gateway verwenden möchten.
- **Allowed IP** (Zugelassene IP): Geben Sie die IP-Adressen an, über die das Gateway von einem entfernten Standort aus verwaltet werden kann. Sollen für die IP-Adressen keine Einschränkungen gelten, klicken Sie auf **All** (Alle). Wenn nur eine einzige IP-Adresse angegeben werden soll, klicken Sie auf **IP address** (IP-Adresse) und geben Sie die IP-Adresse in die entsprechenden Felder ein. Um einen IP-Adressen-Bereich anzugeben, wählen Sie **IP range** (IP-Bereich) aus und geben Sie den IP-Adressen-Bereich in die entsprechenden Felder ein.

**Remote Upgrade** (Remote-Aktualisierung): Mit dieser Funktion kann die Gateway-Firmware von einem entfernten Standort aus über einen TFTP-Server aktualisiert werden. Klicken Sie zum Aktivieren von **Remote Upgrade** (Remote-Aktualisierung) auf **Enable** (Aktivieren).

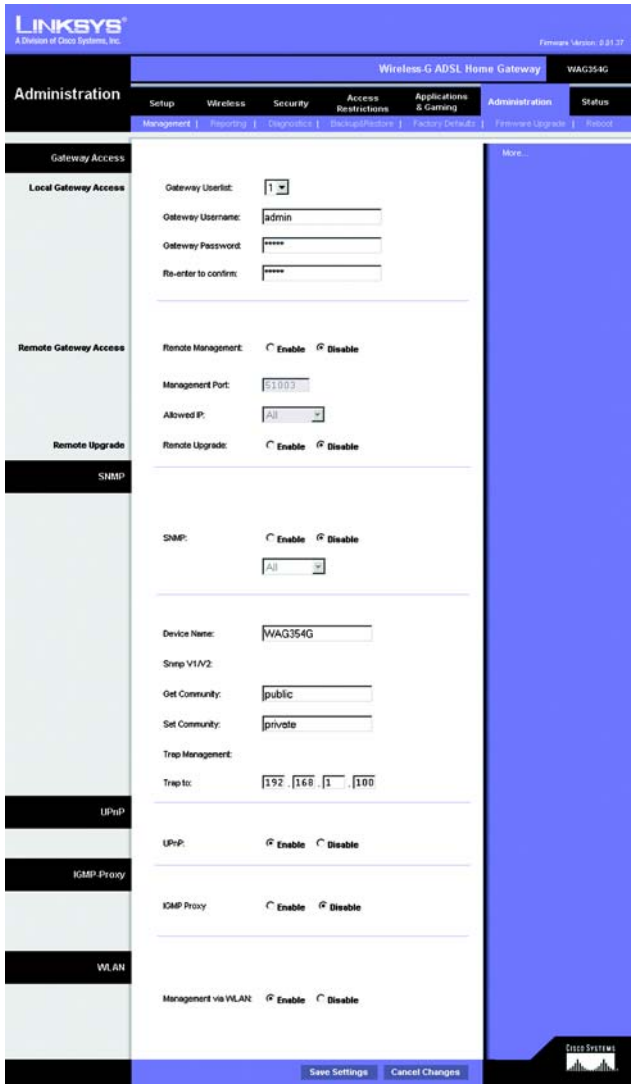



**Abbildung 5-32: Verwaltungsfunktionen**

**Abbildung 5-33: Zugelassene IP bzw. zugelassener IP-Bereich**

### SNMP

**SNMP** ist ein häufig verwendetes Protokoll zur Netzwerküberwachung und -verwaltung. Um **SNMP** zu verwenden, klicken Sie auf **Enabled** (Aktiviert). Um **SNMP** zu deaktivieren, klicken Sie auf **Disabled** (Deaktiviert).

Ist diese Option aktiviert, geben Sie die IP-Adressen ein, denen SNMP-Zugriff gewährt werden soll. Wählen Sie **All** (Alle) aus, wenn für die IP-Adressen keine Einschränkungen gelten sollen, **IP address** (IP-Adresse), wenn Sie eine einzelne IP-Adresse angeben möchten, oder **IP range** (IP-Bereich), wenn Sie einen IP-Adressen-Bereich angeben möchten.

- **Device Name** (Gerätename): Geben Sie den Gateway-Namen ein.
- **SNMP V1/V2**: **Get Community** (Gemeinschaft abrufen): Geben Sie das Passwort ein, mit dem der schreibgeschützte Zugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Set Community** (Gemeinschaft einrichten): Geben Sie das Passwort ein, mit dem der Schreib-/Lesezugriff auf die SNMP-Informationen des Gateways gewährt wird.
- **Trap Management**: **Trap to** (Trap-Verwaltung: Trap-Ziel): Geben Sie die IP-Adresse des entfernten Host-Computers ein, der die Trap-Nachrichten erhalten wird.

### UPnP

Mit UPnP kann das Gateway unter Windows ME und XP automatisch für verschiedene Internetanwendungen, wie z. B. Internet-Spiele oder Videokonferenzen, konfiguriert werden.

- **UPnP**: Um **UPnP** zu verwenden, klicken Sie auf **Enable** (Aktivieren). Klicken Sie andernfalls auf **Disable** (Deaktivieren).

### IGMP-Proxy

Wenn die Multimediaanwendung oder das Gerät hinter dem Gateway nicht ordnungsgemäß funktioniert, können Sie **IGMP-Proxy** aktivieren, um Multicast-Datenverkehr durch das Gateway zuzulassen.

- **IGMP Proxy** (IGMP-Proxy): Klicken Sie auf **Enable** (Aktivieren), um diese Funktion zu verwenden. Andernfalls klicken Sie auf **Disable** (Deaktivieren).

### WLAN

- **Management via WLAN** (Verwaltung über WLAN): Mit dieser Funktion kann das Gateway über einen Wireless-Computer des lokalen Netzwerks verwaltet werden, wenn sich dieser beim webbasierten Dienstprogramm des Gateways anmeldet.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

## Registerkarte „Reporting“ (Berichtaufzeichnung)

Im Fenster *Reporting* (Berichtaufzeichnung) wird ein Protokoll angezeigt, in dem alle eingehenden und ausgehenden URLs bzw. IP-Adressen für die Internetverbindung aufgeführt sind. Über diese Registerkarte stehen auch Protokolle für VPN- und Firewall-Ereignisse zur Verfügung.

**Abbildung 5-34: Berichtaufzeichnung**

### Berichtaufzeichnung

- **Log** (Protokoll): Um die Berichtaufzeichnung zu aktivieren, klicken Sie auf **Enabled** (Aktiviert).
- **Logviewer IP Address** (Logviewer-IP-Adresse): Geben Sie die IP-Adresse des Computers ein, von dem Protokolle empfangen werden. Zum Anzeigen dieser Protokolle ist die Logviewer-Software erforderlich. Diese Software kann kostenlos unter www.linksys.com heruntergeladen werden.

### E-Mail-Warnungen

- **Email Alerts** (E-Mail-Warnungen): Um E-Mail-Warnungen zu aktivieren, klicken Sie auf die Option **Enabled** (Aktiviert).
- **Denial of Service Thresholds** (DoS-Schwellenwerte): Geben Sie die Anzahl der DoS-Angriffe (*Denial of Service*) ein, durch die eine E-Mail-Warnung ausgelöst werden soll.
- **SMTP Mail Server** (SMTP Mail-Server): Geben Sie die IP-Adresse des SMTP-Servers ein.
- **E-Mail Address for Alert Logs** (E-Mail-Adresse für Warnungsprotokolle): Geben Sie die E-Mail-Adresse ein, an die Warnungsprotokolle gesendet werden sollen.
- **Return E-Mail address** (E-Mail-Antwortadresse): Geben Sie die Antwortadresse für die E-Mail-Warnungen ein.

Um Protokolle anzuzeigen, klicken Sie auf die Schaltfläche **View Logs** (Protokolle anzeigen). Es wird ein neues Fenster angezeigt. Sie können das anzuzeigende Protokoll aus dem Dropdown-Menü auswählen. Klicken Sie auf die Schaltfläche **Clear** (Löschen), um die Protokollinformationen zu löschen. Klicken Sie auf die Schaltfläche **pageRefresh** (Seite aktualisieren), um die Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Previous Page** (Vorherige Seite), um zur vorherigen Informationsseite zu wechseln. Klicken Sie auf die Schaltfläche **Next Page** (Nächste Seite), um zur nächsten Informationsseite zu wechseln.

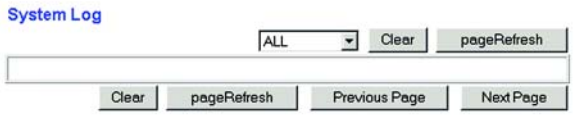



**Abbildung 5-35: Systemprotokoll**

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

## Registerkarte „Diagnostics“ (Diagnose)

### Ping-Test

Ping-Test-Parameter

- **Ping Target IP** (Ping-Ziel-IP-Adresse): Geben Sie die IP-Adresse ein, für die Pings durchgeführt werden sollen. Dies kann eine lokale IP-Adresse (LAN) oder eine Internet-IP-Adresse (WAN) sein.
- **Ping Size** (Ping-Größe): Geben Sie die Größe des Pakets an.
- **Number of Pings** (Anzahl der Pings): Geben Sie an, wie oft die Pings durchgeführt werden sollen.
- **Ping Interval** (Ping-Intervall): Geben Sie den Ping-Intervall (wie oft Pings für die Ziel-IP-Adresse durchgeführt werden sollen) in Millisekunden ein.
- **Ping Timeout** (Ping-Wartezeit): Geben Sie die Ping-Wartezeit (Zeitraum, nach dem der Ping-Test abläuft) in Millisekunden ein.

Klicken Sie auf die Schaltfläche **Start Test** (Test starten), um den Ping-Test zu starten.

- **Ping Result** (Ping-Ergebnisse): In dieser Zeile werden die Ergebnisse des Ping-Tests angezeigt.

Nachdem Sie die Änderungen auf dieser Registerkarte vorgenommen haben, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um diese Änderungen zu übernehmen. Um Ihre Änderungen rückgängig zu machen, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

**Abbildung 5-36: Ping-Test**

## Registerkarte „Backup & Restore“ (Sichern & Wiederherstellen)

Mit der Registerkarte **Backup & Restore** (Sichern & Wiederherstellen) können Sie eine Sicherungskopie der Konfigurationsdatei des Gateways erstellen und diese wiederherstellen.

### Konfiguration sichern

Klicken Sie zum Erstellen einer Sicherungskopie der Konfigurationsdatei des Gateways auf die Schaltfläche **Backup** (Sichern). Befolgen Sie dann die Anweisungen auf dem Bildschirm.

### Konfiguration wiederherstellen

Klicken Sie zum Wiederherstellen der Konfigurationsdatei des Gateways auf die Schaltfläche **Browse** (Durchsuchen). Befolgen Sie dann die Anweisungen auf dem Bildschirm, um nach der Datei zu suchen. Wenn Sie die Datei gefunden haben, klicken Sie auf die Schaltfläche **Restore** (Wiederherstellen).

**Abbildung 5-37: Sichern & Wiederherstellen**

## Registerkarte „Factory Defaults“ (Werkseinstellungen)

**Restore Factory Defaults** (Werkseinstellungen wiederherstellen): Wenn Sie das Gateway auf die Werkseinstellungen zurücksetzen möchten (Ihre Einstellungen werden dabei nicht beibehalten), klicken Sie auf **Yes** (Ja).

Um den Wiederherstellungsvorgang zu starten und die Einstellungen zu speichern, klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern) bzw. auf **Cancel Changes** (Änderungen verwerfen), um Ihre Änderungen zu verwerfen.

**Abbildung 5-38: Werkseinstellungen**

## Registerkarte „Firmware Upgrade“ (Aktualisieren der Firmware)

Mit dem Gateway können Sie Firmware für die LAN-Seite (Netzwerkseite) des Gateways aktualisieren.

### Aktualisieren aus dem LAN

So aktualisieren Sie die Gateway-Firmware aus dem LAN:

1. Laden Sie die Datei zum Aktualisieren der Gateway-Firmware unter www.linksys.com herunter.
1. Extrahieren Sie die Datei auf Ihrem Computer.
1. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der Firmware-Aktualisierungsdatei zu suchen.
2. Doppelklicken Sie auf die Firmware-Datei, die Sie heruntergeladen und extrahiert haben.
3. Klicken Sie auf die Schaltfläche **Upgrade** (Aktualisieren), und befolgen Sie die Anweisungen auf dem Bildschirm.

Um die Aktualisierung der Firmware abzubrechen, klicken Sie auf die Schaltfläche **Cancel Upgrade** (Aktualisierung abbrechen).

**Abbildung 5-39: Firmware aktualisieren**

## Registerkarte „Reboot“ (Neustart)

In diesem Fenster können Sie einen Warm- oder Kaltstart für das Gateway ausführen. Für die meisten Situationen empfiehlt sich ein Kaltstart. Ein Warmstart ist mit einem Neustart des Computers vergleichbar, bei dem der Computer nicht physisch ausgeschaltet wird.

### Neustart

**Reboot Mode** (Neustart-Modus): Um Ihr Gateway neu zu starten, wählen Sie **Hard** (Kaltstart) oder **Soft** (Warmstart) aus. Um das Gateway aus- und wieder einzuschalten, wählen Sie die Option **Hard** (Kaltstart). Um das Gateway neu zu starten, ohne es auszuschalten, wählen Sie die Option **Soft** (Warmstart) aus.

Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um den Neustart zu starten. Wenn ein Fenster angezeigt wird, in dem Sie gefragt werden, ob Sie für das Gateway wirklich einen Neustart ausführen möchten, klicken Sie auf **OK**.

Wenn Sie den Neustart abbrechen möchten, klicken Sie auf die Schaltfläche **Cancel Changes** (Änderungen verwerfen).

**Abbildung 5-40: Neustart**

# Registerkarte „Status“

## Registerkarte „Gateway“

In diesem Fenster werden Informationen zum Gateway und zu seiner Internetverbindung angezeigt.

### Gateway-Informationen

In diesem Bereich wird die Version der Gateway-Firmware, die MAC-Adresse und die aktuelle Uhrzeit angezeigt.

### Internetverbindung

In diesem Bereich werden folgende Informationen angezeigt: Verbindung, Anmeldetyp, Schnittstelle, IP-Adresse, Subnetzmaske, Standard-Gateway, IP-Adressen der DNS-Server 1, 2 und 3 sowie die WINS-Adresse.

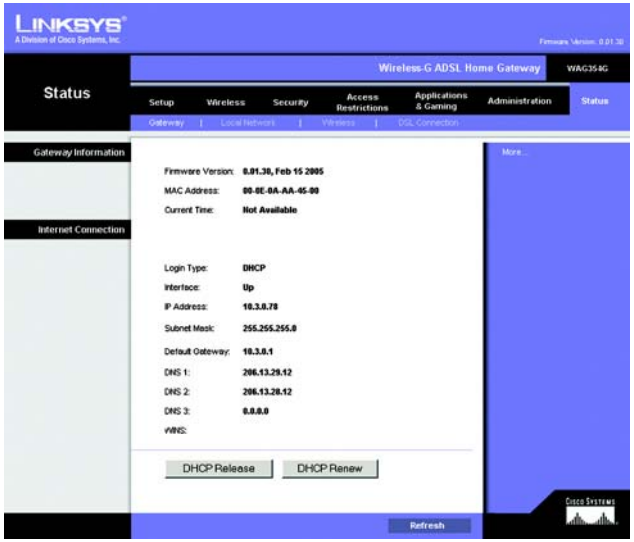



**Abbildung 5-41: Gateway**

**DHCP Renew** (DHCP erneuern): Klicken Sie auf die Schaltfläche **DHCP Renew** (DHCP erneuern), um die aktuelle IP-Adresse des Gateways durch eine neue IP-Adresse zu ersetzen.

**DHCP Release** (DHCP löschen): Klicken Sie auf die Schaltfläche **DHCP Release** (DHCP löschen), um die aktuelle IP-Adresse des Gateways zu löschen.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.

## Registerkarte „Local Network“ (Lokales Netzwerk)

Im Bereich **Local Network** (Lokales Netzwerk) sind Angaben zur lokalen MAC-Adresse, IP-Adresse, Subnetzmaske, zum DHCP-Server sowie zur Start- und End-IP-Adresse aufgeführt. Um die DHCP-Client-Tabelle anzuzeigen, klicken Sie auf die Schaltfläche **DHCP Clients Table** (DHCP-Client-Tabelle). Klicken Sie zum Anzeigen der ARP/RARP-Tabelle auf die Schaltfläche **ARP/RARP Table** (ARP/RARP-Tabelle).

**DHCP Client Table** (DHCP-Client-Tabelle): Im Bereich **DHCP Active IP Table** (DHCP - Tabelle zur aktiven IP-Adresse) werden die aktuellen DHCP-Client-Daten angezeigt. Zu diesen Angaben zählen der Computername, die IP-Adresse, die MAC-Adresse und der Zeitpunkt, zu dem die dynamische IP-Adresse für die Wireless-Clients, die den DHCP-Server nutzen, abläuft. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Um einen Client vom DHCP-Server zu löschen, wählen Sie den entsprechenden Client aus und klicken Sie anschließend auf die Schaltfläche **Delete** (Löschen). Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Local Network* (Lokales Netzwerk) zurückzukehren.

**ARP/RARP Table** (ARP/RARP-Tabelle): Im Bereich **ARP/RARP Table** (ARP/RARP-Tabelle) sind die aktuellen Angaben für die Clients des lokalen Netzwerks aufgeführt, die eine ARP-Anfrage an das Gateway gesendet haben. Es werden die entsprechenden IP-Adressen und MAC-Adressen aufgeführt. (Diese Daten werden im temporären Speicher gespeichert und ändern sich in regelmäßigen Abständen.) Bei einer ARP-Anfrage handelt es sich um eine Anfrage, mit der das Gateway die MAC-Adressen von Clients mit IP-Adressen anfragt, um IP-Adressen den entsprechenden MAC-Adressen zuordnen zu können. Bei RARP geht der Vorgang im Vergleich zu ARP umgekehrt vonstatten. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Local Network* (Lokales Netzwerk) zurückzukehren.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.

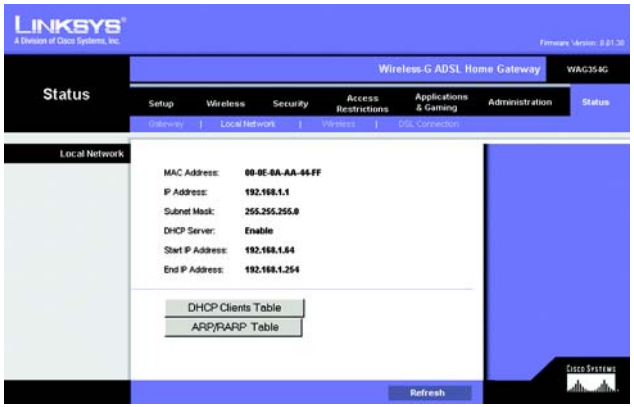



**Abbildung 5-42: Lokales Netzwerk**

**Abbildung 5-43: DHCP - Tabelle zur aktiven IP-Adresse**

**Abbildung 5-44: ARP/RARP-Tabelle**

## Registerkarte „Wireless“

Im Bereich der Wireless-Netzwerkinformationen sind Angaben zu Wireless-Firmware-Version, MAC-Adresse, Modus, SSID, DHCP-Server, Kanal sowie zur Verschlüsselungsfunktion aufgeführt.

Klicken Sie auf die Schaltfläche **Wireless Clients Connected** (Angeschlossene Wireless-Clients), um eine Liste der Wireless-Clients anzuzeigen, die an das Gateway angeschlossen sind. Gleichzeitig werden die entsprechenden Computernamen, IP-Adressen und MAC-Adressen angezeigt. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren. Klicken Sie auf die Schaltfläche **Close** (Schließen), um zum Fenster *Wireless* zurückzukehren.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.

**Abbildung 5-45: Wireless**

**Abbildung 5-46: Netzwerk-Computer**

## Registerkarte „DSL Connection“ (DSL-Verbindung)

In diesem Fenster werden Informationen zur DSL- und PVC-Verbindung angezeigt.

### DSL-Status

In diesem Bereich werden folgende Informationen angezeigt: DSL-Status, DSL-Modulationsmodus, DSL-Pfadmodus, Downstream-Rate, Upstream-Rate, Downstream-Grenze, Upstream-Grenze, Downstream-Verbindungsabschwächung, Upstream-Verbindungsabschwächung, Downstream-Übertragungsleistung und Upstream-Übertragungsleistung.

### PVC-Verbindung

In diesem Bereich werden folgende Informationen angezeigt: Kapselungsmethode, Multiplexing, QoS, PCR-Rate, SCR-Rate, Automatisch erkennen, VPI, VCI, Aktiviert-Status und PVC-Status.

Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die angezeigten Informationen zu aktualisieren.

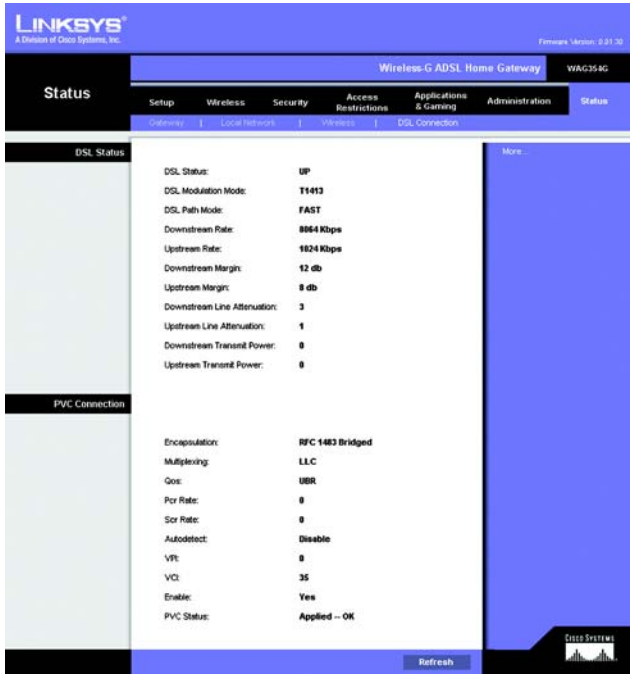



**Abbildung 5-47: DSL-Verbindung**

# Anhang A: Fehlerbehebung

Dieser Anhang besteht aus zwei Teilen: „Behebung häufig auftretender Probleme“ und „Häufig gestellte Fragen“. Er enthält Lösungsvorschläge zu Problemen, die während der Installation und des Betriebs des Gateways auftreten können. Lesen Sie sich zur Fehlerbehebung die unten aufgeführten Beschreibungen durch. Wenn hier kein Lösungsvorschlag zu Ihrem Problem aufgeführt ist, finden Sie weitere Informationen auf der Website von Linksys unter www.linksys.com/international.

## Behebung häufig auftretender Probleme

***1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?***

Führen Sie die folgenden Schritte aus, um einem Computer eine statische IP-Adresse zuzuweisen:

- Für Benutzer von Windows 98 und ME:
  1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf die Option **Netzwerk**.
  2. Wählen Sie im Feld **Die folgenden Netzwerkkomponenten sind installiert** die mit dem Ethernet-Adapter verbundene Option **TCP/IP->** aus. Falls nur ein Ethernet-Adapter installiert ist, wird nur in einer Zeile „TCP/IP“ ohne Verknüpfung mit einem Ethernet-Adapter aufgeführt. Wählen Sie den Eintrag aus, und klicken Sie auf die Schaltfläche **Eigenschaften**.
  3. Wählen Sie im Fenster für die TCP/IP-Eigenschaften in der Registerkarte **IP-Adresse** die Option **IP-Adresse festlegen** aus. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird. Vergewissern Sie sich, dass für jeden Computer bzw. jedes Netzwerkgerät eine eindeutige IP-Adresse verwendet wird.
  4. Klicken Sie auf die Registerkarte **Gateway** und geben Sie 192.168.1.1 ein, wenn die Eingabeaufforderung für das neue Gateway angezeigt wird (dies ist die Standard-IP-Adresse für das Gateway). Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Eingabe zu übernehmen.
  5. Klicken Sie auf die Registerkarte **DNS**, und stellen Sie sicher, dass die Option **DNS** aktiviert ist. Geben Sie den Host- und den Domänennamen ein (z. B. „Johann“ als Hostname und „home“ als Domänenname). Geben Sie den DNS-Eintrag ein, den Sie von Ihrem ISP erhalten haben. Falls Sie keine DNS-IP-Adresse von Ihrem ISP erhalten haben, wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
  6. Klicken Sie im Fenster für die TCP/IP-Eigenschaften auf **OK**, und klicken Sie anschließend auf die Schaltfläche **Schließen** bzw. die Schaltfläche **OK**, um das Fenster **Netzwerk** zu schließen.
  7. Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.
- Für Benutzer von Windows 2000:
  1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Netzwerk- und DFÜ-Verbindungen**.

2. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
3. Wählen Sie im Feld **Aktivierte Komponenten werden von dieser Verbindung verwendet** die Option **Internetprotokoll (TCP/IP)** aus, und klicken Sie auf die Schaltfläche **Eigenschaften**. Wählen Sie die Option **Folgende IP-Adresse verwenden** aus.
4. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
5. Geben Sie für die Subnetzmaske den Eintrag 255.255.255.0 ein.
6. Geben Sie für das Standardgateway den Eintrag 192.168.1.1 ein (die Standard-IP-Adresse des Gateways).
7. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
8. Klicken Sie im Fenster **Internetprotokolleigenschaften (TCP/IP)** auf die Schaltfläche **OK** sowie im Fenster **Eigenschaften von LAN-Verbindung** auf die Schaltfläche **OK**.
9. Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.

- Für Benutzer von Windows XP:
  Die folgenden Anweisungen gelten, wenn Sie Windows XP mit der Standard-Benutzeroberfläche ausführen. Wenn Sie die klassische Benutzeroberfläche verwenden (bei der die Symbole und Menüs wie in vorherigen Windows-Versionen aussehen), befolgen Sie die Anweisungen für Windows 2000.
  1. Klicken Sie auf **Start** und **Systemsteuerung**.
  2. Klicken Sie auf das Symbol **Netzwerk- und Internetverbindungen** und dann auf **Netzwerkverbindungen**.
  3. Klicken Sie mit der rechten Maustaste auf die LAN-Verbindung, die mit dem von Ihnen verwendeten Ethernet-Adapter verknüpft ist, und wählen Sie die Option **Eigenschaften** aus.
  4. Wählen Sie im Feld **Diese Verbindung verwendet folgende Elemente** die Option **Internetprotokoll (TCP/IP)**. Klicken Sie auf die Schaltfläche **Eigenschaften**.
  5. Geben Sie eine eindeutige IP-Adresse ein, die von keinem anderen an das Gateway angeschlossenen Computer im Netzwerk verwendet wird.
  6. Geben Sie für die Subnetzmaske den Eintrag 255.255.255.0 ein.
  7. Geben Sie für das Standardgateway den Eintrag 192.168.1.1 ein (die Standard-IP-Adresse des Gateways).
  8. Wählen Sie im unteren Fensterbereich die Option **Folgende DNS-Serveradressen verwenden** aus, und geben Sie den bevorzugten und den alternativen DNS-Server ein (diese Angaben erhalten Sie von Ihrem ISP). Wenden Sie sich an Ihren ISP bzw. sehen Sie auf dessen Website nach, um diese Informationen zu erhalten.
  9. Klicken Sie im Fenster **Internetprotokolleigenschaften (TCP/IP)** auf die Schaltfläche **OK**. Klicken Sie im Fenster **Eigenschaften von LAN-Verbindung** auf die Schaltfläche **OK**.

***2. Ich möchte meine Internetverbindung prüfen.***

A. Überprüfen Sie Ihre TCP/IP-Einstellungen.

Für Benutzer von Windows 98, ME, 2000 und XP:

- Weitere Informationen finden Sie in der Windows-Hilfe. Stellen Sie sicher, dass in den Einstellungen die Option **IP-Adresse automatisch beziehen** aktiviert ist.

Für Benutzer von Windows NT 4.0:

- Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf das Symbol **Netzwerk**.
- Klicken Sie auf die Registerkarte **Protokoll**, und doppelklicken Sie auf **TCP/IP-Protokoll**.
- Wenn das Fenster angezeigt wird, stellen Sie sicher, dass Sie den richtigen Adapter als Ihren Ethernet-Adapter und die Option **IP-Adresse von einem DHCP-Server beziehen** ausgewählt haben.
- Klicken Sie im Fenster mit den TCP/IP-Protokolleigenschaften auf die Schaltfläche **OK** und im Fenster **Netzwerk** auf die Schaltfläche **Schließen**.
- Wenn Sie dazu aufgefordert werden, starten Sie Ihren Computer neu.

B. Öffnen Sie eine Eingabeaufforderung.

Für Benutzer von Windows 98 und ME:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie in das Feld **Öffnen** den Eintrag **command** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

Für Benutzer von Windows NT, 2000 und XP:

- Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen** den Eintrag **cmd** ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**. Geben Sie in die Eingabeaufforderung den Eintrag **ping 192.168.1.1** ein, und drücken Sie die Eingabetaste.
- Wenn Sie eine Antwort erhalten, kommuniziert der Computer mit dem Gateway.
- Wenn Sie KEINE Antwort erhalten, überprüfen Sie die Kabelverbindung und stellen Sie sicher, dass in den TCP/IP-Einstellungen für den Ethernet-Adapter die Option **IP-Adresse automatisch beziehen** aktiviert ist.

C. Geben Sie in die Eingabeaufforderung den Eintrag **ping** gefolgt von Ihrer Internet- bzw. WAN-IP-Adresse ein, und drücken Sie die Eingabetaste. Die Internet- bzw. WAN-IP-Adresse wird im Statusfenster des webbasierten Dienstprogramms des Gateways angezeigt. Beispiel: Wenn Ihre Internet- bzw. WAN-IP-Adresse 1.2.3.4 lautet, müssen Sie den Eintrag **ping 1.2.3.4** eingeben und anschließend die Eingabetaste drücken.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Gateway verbunden.
- Wenn Sie KEINE Antwort erhalten, geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

D. Geben Sie in die Eingabeaufforderung den Eintrag **ping www.yahoo.com** ein, und drücken Sie die Eingabetaste.

- Wenn Sie eine Antwort erhalten, ist Ihr Computer mit dem Internet verbunden. Wenn Sie KEINE Website öffnen können, geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.
- Wenn Sie KEINE Antwort erhalten, kann ein Verbindungsproblem vorliegen. Geben Sie den Ping-Befehl über einen anderen Computer ein, um dadurch sicherzustellen, dass das Problem nicht vom ersten Computer verursacht wird.

***3. Mit meiner Internetverbindung erhalte ich keine IP-Adresse im Internet.***

- Lesen Sie sich den oben aufgeführten Abschnitt „2. Ich möchte meine Internetverbindung prüfen“ durch, und überprüfen Sie anhand dessen Ihre Verbindung.
  1. Stellen Sie sicher, dass Sie die korrekten Einstellungen für die Internetverbindung verwenden. Wenden Sie sich an Ihren ISP, um die Art Ihrer Internetverbindung zu überprüfen: RFC 1483 Bridged (RFC 1483-Überbrückung), RFC 1483 Routed (RFC 1483-Übertragung), RFC 2516 PPPoE oder RFC 2364 PPPoA. Weitere Einzelheiten zu den Einstellungen für die Internetverbindung finden Sie in „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“ im Abschnitt zur Registerkarte **Setup** (Einrichten).
  2. Stellen Sie sicher, dass Sie das richtige Kabel verwenden. Überprüfen Sie, ob in der Spalte für das Gateway die ADSL-LED konstant leuchtet.
  3. Stellen Sie sicher, dass das an den ADSL-Port Ihres Gateways angeschlossene Kabel in die Wandbuchse der ADSL-Verbindung eingesteckt ist. Überprüfen Sie, ob in der Statusseite des webbasierten Dienstprogramms des Gateways eine gültige IP-Adresse Ihres ISP aufgeführt ist.
  4. Schalten Sie den Computer und das Gateway aus. Warten Sie 30 Sekunden, und schalten Sie dann das Gateway und den Computer wieder ein. Überprüfen Sie, ob im webbasierten Dienstprogramm des Gateways auf der Registerkarte **Status** eine IP-Adresse angezeigt wird.

***4. Ich kann auf die Setup-Seite des webbasierten Dienstprogramms des Gateways nicht zugreifen.***

- Informationen zur Überprüfung einer ordnungsgemäßen Verbindung des Computers mit dem Gateway finden Sie unter „2. Ich möchte meine Internetverbindung prüfen“.
  1. Informationen zur Überprüfung, ob Ihr Computer eine IP-Adresse, eine Subnetzmaske, ein Gateway und einen DNS besitzt, finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
  2. Legen Sie eine statische IP-Adresse für Ihren Computer fest. Weitere Informationen hierzu finden Sie unter „1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?“.
  3. Folgen Sie den Anweisungen unter „10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?

***5. Mein VPN (Virtual Private Network) funktioniert nicht über das Gateway.***

Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf, und öffnen Sie die Registerkarte **Security** (Sicherheit). Stellen Sie sicher, dass Sie die Option **IPSec Passthrough** (IPSec-Passthrough) und/oder **PPTP Passthrough** (PPTP-Passthrough) aktiviert haben.

- VPNs, in denen IPSec mit der ESP-Authentifizierung (*Encapsulation Security Payload*, auch als Protokoll 50 bezeichnet) verwendet wird, funktionieren einwandfrei. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen. Je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.
- VPNs, in denen IPSec und AH (*Authentication Header*, auch als Protokoll 51 bezeichnet) verwendet werden, sind mit dem Gateway nicht kompatibel. Die Verwendung von AH ist aufgrund gelegentlicher Inkompatibilität mit dem NAT-Standard beschränkt.

- Ändern Sie die IP-Adresse des Gateways auf ein anderes Subnetz, so dass Konflikte zwischen der IP-Adresse des VPNs und Ihrer lokalen IP-Adresse vermieden werden. Wenn Ihr VPN-Server beispielsweise die IP-Adresse 192.168.1.X zuweist (wobei „X“ für eine Zahl zwischen 1 und 254 steht) und die IP-Adresse Ihres LANs 192.168.1.X lautet (wobei „X“ mit der in der IP-Adresse des VPNs verwendeten Zahl identisch ist), werden Informationen vom Gateway u. U. nicht richtig übertragen. Zur Problembehebung ändern Sie die IP-Adresse des Gateways in 192.168.2.1. Ändern Sie die IP-Adresse des Gateways im webbasierten Dienstprogramm auf der Registerkarte **Setup** (Einrichtung).
- Wenn Sie einem Computer oder einem anderen Gerät in Ihrem Netzwerk eine statische IP-Adresse zugewiesen haben, müssen Sie seine IP-Adresse dementsprechend in 192.168.2.Y (wobei „Y“ für eine Zahl zwischen 1 und 254 steht) ändern. Beachten Sie, dass jede IP-Adresse im Netzwerk eindeutig sein muss.
- Bei Ihrem VPN ist es u. U. erforderlich, dass Port 500/UDP-Pakete an den Computer übertragen werden, der mit dem IPSec-Server verbunden ist. Details hierzu finden Sie unter „7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internet-Anwendungen verwenden.“
- Weitere Informationen finden Sie auf der Website von Linksys unter www.linksys.com/international.

***6. Wie richte ich einen Server hinter dem Gateway ein und gebe ihn für alle Benutzer frei?***

Um einen Server als Web-, FTP- oder Mail-Server zu verwenden, muss Ihnen die jeweils verwendete Anschlussnummer bekannt sein. Beispiel: Port 80 (HTTP) wird für Webserver, Port 21 (FTP) für FTP-Server und Port 25 (SMTP Ausgang) sowie Port 110 (POP3 Eingang) für Mail-Server verwendet. Weitere Informationen finden Sie in der Dokumentation des installierten Servers.

- Befolgen Sie die hier aufgeführten Schritte, um die Port-Weiterleitung über das webbasierte Dienstprogramm des Gateways einzurichten. Im Folgenden finden Sie Anweisungen zum Einrichten von Web-, FTP- und Mail-Servern.
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
  2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
  3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Wenn Sie beispielsweise einen Webserver verwenden, legen Sie den Bereich zwischen 80 und 80 fest.
  4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
  5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert 100 in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Aktivieren**. Beachten Sie folgendes Beispiel:

| Benutzerdefinierte Anwendung | Externer Anschluss | TCP | UDP | IP-Adresse | Aktivieren |
|---|---|---|---|---|---|
| Webserver | 80 bis 80 | X | | 192.168.1.100 | X |
| FTP-Server | 21 bis 21 | X | | 192.168.1.101 | X |
| SMTP (Ausgang) | 25 bis 25 | X | | 192.168.1.102 | X |
| POP3 (Eingang) | 110 bis 110 | X | | 192.168.1.102 | X |

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

***7. Ich möchte das Hosting für Online-Spiele einrichten bzw. weitere Internetanwendungen verwenden.***

Zum Verwenden von Online-Spielen oder Internetanwendungen ist i. d. R. keine Port-Weiterleitung bzw. kein DMZ-Hosting notwendig. In einigen Fällen müssen Sie u. U. das Hosting für Online-Spiele oder Internetanwendungen anwenden. Dafür müssen Sie das Gateway so einrichten, dass eingehende Datenpakete oder Daten an einen bestimmten Computer geliefert werden. Dies trifft auch auf die verwendeten Internetanwendungen zu. Sie erhalten Informationen zu den zu verwendenden Anschlussdiensten auf der Website des betreffenden Online-Spiels bzw. der Anwendung, das bzw. die Sie verwenden möchten. Führen Sie diese Schritte aus, um ein Hosting für ein Online-Spiel auszuführen bzw. um eine bestimmte Internetanwendung zu verwenden:

1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **Port Range Forwarding** (Weiterleitung an einen Anschlussbereich) auf.
2. Geben Sie für die benutzerdefinierte Anwendung einen beliebigen Namen ein.
3. Geben Sie den Bereich der externen Anschlüsse für den verwendeten Dienst an. Um beispielsweise Unreal Tournament (UT) auszuführen, müssen Sie den Bereich von 7777 bis 27900 eingeben.
4. Überprüfen Sie, welches Protokoll (TCP und/oder UDP) verwendet werden soll.
5. Geben Sie die IP-Adresse des Ziel-Computers bzw. -Netzwerkgeräts für den Anschluss-Server ein. Beispiel: Wenn die IP-Adresse für den Ethernet-Adapter des Webservers 192.168.1.100 lautet, geben Sie den Wert 100 in das dafür vorgesehene Feld ein. Weitere Informationen zum Ermitteln von IP-Adressen finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.
6. Aktivieren Sie für die zu verwendenden Anschlussdienste die Option **Aktivieren**. Beachten Sie folgendes Beispiel:

| Benutzerdefinierte Anwendung | Externer Anschluss | TCP | UDP | IP-Adresse | Aktivieren |
|---|---|---|---|---|---|
| UT | 7777 bis 27900 | X | X | 192.168.1.100 | X |
| Halflife | 27015 bis 27015 | X | X | 192.168.1.105 | X |
| PCAnywhere | 5631 bis 5631 | | X | 192.168.1.102 | X |
| VPN/IPSEC | 500 bis 500 | | X | 192.168.1.100 | X |

Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

***8. Weder Internetspiele, Internetserver noch Internetanwendungen funktionieren.***

Falls Sie Schwierigkeiten haben, Internetspiele, -server und -anwendungen zu verwenden, verbinden Sie einen Computer über das DMZ-Hosting (*DeMilitarized Zone*) mit dem Internet. Diese Option ist verfügbar, wenn für eine Anwendung zu viele Ports erforderlich sind oder Sie nicht sicher sind, welchen Anschlussdienst Sie verwenden sollen. Stellen Sie sicher, dass alle Weiterleitungseinträge deaktiviert sind, um das DMZ-Hosting erfolgreich zu verwenden, da das Forwarding Vorrang vor dem DMZ-Hosting hat. (Mit anderen Worten: In dem Gateway eingehende Daten werden zuerst hinsichtlich ihrer Forwarding-Einstellungen überprüft. Falls die Daten von einer Portnummer eingehen, für die keine Port-Weiterleitung aktiviert ist, sendet das Gateway die Daten an einen beliebigen Computer oder ein beliebiges Netzwerkgerät, der bzw. das für DMZ-Hosting festgelegt wurde.)

- Führen Sie folgende Schritte aus, um DMZ-Hosting festzulegen:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Rufen Sie unter **Applications and Gaming** (Anwendungen und Spiele) die Registerkarte **DMZ** auf. Wählen Sie **Enabled** (Aktiviert) aus, und geben Sie die IP-Adresse des Computers ein.
  2. Überprüfen Sie die Seiten zur Port-Weiterleitung, und deaktivieren bzw. entfernen Sie die Einträge zum Forwarding. Speichern Sie diese Informationen, falls Sie sie zu einem späteren Zeitpunkt verwenden möchten.
- Klicken Sie nach Abschluss der Konfiguration auf die Schaltfläche **Save Settings** (Einstellungen speichern).

***9. Ich habe das Passwort vergessen bzw. die Aufforderung zur Eingabe des Passworts wird jedes Mal angezeigt, wenn ich die Einstellungen für das Gateway speichere.***

- Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste 10 Sekunden lang gedrückt halten. Wenn Sie immer noch bei jedem Speichern der Einstellungen zur Eingabe des Passworts aufgefordert werden, führen Sie die folgenden Schritte aus:
  1. Rufen Sie über **http://192.168.1.1** bzw. über die IP-Adresse des Gateways das webbasierte Dienstprogramm des Gateways auf. Geben Sie den Standardbenutzernamen und das Standardpasswort **admin** ein, und rufen Sie unter **Administration** (Verwaltung) die Registerkarte **Management** (Verwaltungsfunktionen) auf.
  2. Geben Sie in das Feld für das Gateway-Passwort ein anderes Passwort ein. Geben Sie anschließend das gleiche Passwort in das zweite Feld ein, um es dadurch zu bestätigen.
  3. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern).

***10. Wie kann ich als PPPoE-Benutzer die Proxy-Einstellungen bzw. das Popup-Fenster für DFÜ-Verbindungen entfernen?***

Wenn Sie Proxy-Einstellungen verwenden, müssen Sie diese auf Ihrem Computer deaktivieren. Da es sich bei dem Gateway um das Gateway für die Internetverbindung handelt, benötigt der Computer keine Proxy-Einstellungen für den Zugriff auf das Internet. Führen Sie die folgenden Anweisungen aus, um sicherzustellen, dass Sie keine Proxy-Einstellungen verwenden und der verwendete Browser direkt eine Verbindung mit dem LAN herstellt.

- Für Benutzer von Microsoft Internet Explorer 5.0 oder höher:
  1. Klicken Sie auf **Start**, **Einstellungen** und **Systemsteuerung**. Doppelklicken Sie auf **Internetoptionen**.
  2. Klicken Sie auf die Registerkarte **Verbindungen**.
  3. Klicken Sie auf die Schaltfläche **LAN-Einstellungen**, und deaktivieren Sie alle aktivierten Optionen.
  4. Klicken Sie auf die Schaltfläche **OK**, um zum vorherigen Fenster zu wechseln.
  5. Aktivieren Sie die Option **Keine Verbindung wählen**. Dadurch werden alle Popup-Fenster für DFÜ-Verbindungen für PPPoE-Benutzer entfernt.

- Für Benutzer von Netscape 6 oder höher:
  1. Starten Sie **Netscape Navigator**, und klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**.
  2. Stellen Sie sicher, dass in diesem Fenster die Option **Direkte Verbindung zum Internet** ausgewählt ist.
  3. Schließen Sie alle Fenster, um den Vorgang zu beenden.

***11. Ich muss das Gateway auf die Werkseinstellungen zurücksetzen, um den Vorgang noch einmal von vorn zu beginnen.***

Halten Sie die Reset-Taste 10 Sekunden lang gedrückt. Dadurch werden die Interneteinstellungen, das Passwort, die Forwarding-Funktion sowie weitere Einstellungen des Gateways auf die Werkseinstellungen zurückgesetzt. Anders ausgedrückt: Das Gateway greift auf die werkseitigen Konfigurationseinstellungen zurück.

***12. Ich möchte die Firmware aktualisieren.***

Um die aktuellsten Funktionen für Ihre Firmware zu erhalten, gehen Sie auf die internationale Website von Linksys und laden Sie die neueste Firmware unter www.linksys.com/international herunter.

- Führen Sie die folgenden Schritte aus:
  1. Wählen Sie auf der internationalen Website von Linksys unter http://www.linksys.com/international Ihre Region bzw. Ihr Land aus.
  2. Klicken Sie auf die Registerkarte **Products** (Produkte), und wählen Sie das Gateway aus.
  3. Klicken Sie auf der Website des Gateways auf **Firmware**, und laden Sie anschließend die aktuelle Firmware für das Gateway herunter.
  4. Um die Firmware zu aktualisieren, führen Sie die in „Kapitel 5: Konfigurieren des Wireless-G ADSL-Home-Gateways“ im Abschnitt **Administration** (Verwaltung) aufgeführten Schritte durch.

***13. Die Aktualisierung der Firmware ist fehlgeschlagen bzw. die Netzstrom-LED blinkt.***

Die Aktualisierung der Firmware kann aus mehreren Gründen fehlschlagen. Führen Sie diese Schritte aus, um die Firmware zu aktualisieren bzw. das Blinken der Netzstrom-LED zu stoppen:

- Wenn die Aktualisierung der Firmware fehlgeschlagen ist, verwenden Sie das TFTP-Programm (das Programm wurde zusammen mit der Firmware heruntergeladen). Öffnen Sie die zusammen mit der Firmware und dem TFTP-Programm heruntergeladene PDF-Datei, und befolgen Sie die darin aufgeführten Anweisungen.

- Legen Sie eine statische IP-Adresse für Ihren Computer fest. Weitere Informationen hierzu finden Sie unter „1. Wie lege ich eine statische IP-Adresse auf einem Computer fest?“. Verwenden Sie für den Computer die folgenden Einstellungen für die IP-Adresse:
  IP-Adresse: 192.168.1.50
  Subnetzmaske: 255.255.255.0
  Gateway: 192.168.1.1
- Nehmen Sie die Aktualisierung mithilfe des TFTP-Programms oder der Registerkarte **Administration** (Verwaltung) im webbasierten Dienstprogramm des Gateways vor.

***14. Das PPPoE-Protokoll des DSL-Anbieters wird stets unterbrochen.***

PPPoE ist keine dedizierte oder stets aktive Verbindung. Die DSL-Verbindung kann durch den ISP getrennt werden, wenn die Verbindung einige Zeit inaktiv war, ähnlich wie bei einer normalen Telefon-DFÜ-Verbindung zum Internet.

- Es steht eine Setup-Option zur Aufrechterhaltung der Verbindung zur Verfügung. Diese Option funktioniert möglicherweise nicht immer, Sie müssen daher die Verbindung regelmäßig neu herstellen.
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)
  3. Wählen Sie im Setup-Fenster die Option **Keep Alive** (Verbindung aufrechterhalten) aus, und legen Sie für die Option **Redial Period** (Wahlwiederholung) 20 Sekunden fest.
  4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern). Klicken Sie auf die Registerkarte **Status** (Status), und klicken Sie auf Schaltfläche **Connect** (Verbinden).
  5. Möglicherweise wird **Connecting** (Verbindung wird hergestellt) als Anmeldestatus angezeigt. Drücken Sie die F5-Taste, um den Bildschirm zu aktualisieren, bis **Connected** (Verbunden) als Anmeldestatus angezeigt wird.
  6. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.
- Falls die Verbindung erneut unterbrochen wird, führen Sie die Schritte 1 bis 6 aus, um die Verbindung wiederherzustellen.

***15. Ich kann weder auf meine E-Mail noch auf das Internet oder auf das VPN zugreifen, oder ich bekomme nur beschädigte Daten aus dem Internet.***

Sie müssen den Wert für die MTU-Einstellung (*Maximum Transmission Unit*; Maximale Übertragungseinheit) anpassen. Die maximale Übertragungseinheit wird standardmäßig automatisch festgelegt.

- Wenn Sie Schwierigkeiten haben, führen Sie folgende Schritte aus:
  1. Rufen Sie zum Verbinden des Gateways den Web-Browser auf, und geben Sie **http://192.168.1.1** bzw. die IP-Adresse des Gateways ein.
  2. Geben Sie, falls erforderlich, Ihren Benutzernamen und Ihr Passwort ein. (Der Standardbenutzername und das Standardpasswort sind **admin**.)

3. Wählen Sie für die MTU-Option **Manual** (Manuell) aus. Geben Sie in das Feld **Size** (Größe) den Wert 1492 ein.
4. Klicken Sie auf die Schaltfläche **Save Settings** (Einstellungen speichern), um fortzufahren.

- Wenn das Problem weiterhin besteht, ändern Sie den MTU-Wert auf einen anderen Wert. Verwenden Sie aus der folgenden Liste jeweils einen Wert in der angegebenen Reihenfolge, bis Ihr Problem gelöst ist:
  1462
  1400
  1362
  1300

***16. Die Netzstrom-LED leuchtet durchgehend.***

Die Netzstrom-LED leuchtet auf, wenn das Gerät erstmals eingeschaltet wird. Zwischenzeitlich fährt der Computer hoch und wird auf einen ordnungsgemäßen Betrieb hin geprüft. Nach dem Überprüfungsvorgang leuchtet die LED konstant, wodurch der ordnungsgemäße Betrieb angezeigt wird. Wenn die LED immer noch blinkt, funktioniert das Gerät nicht ordnungsgemäß. Führen Sie einen Firmware-Flash durch, indem Sie dem Computer eine statische IP-Adresse zuweisen, und aktualisieren Sie anschließend die Firmware. Verwenden Sie hierfür die folgenden Einstellungen: IP-Adresse: 192.168.1.50, Subnetzmaske: 255.255.255.0.

***17. Bei Eingabe einer URL- oder IP-Adresse erhalte ich eine Meldung, dass eine Zeitüberschreitung vorliegt, bzw. die Aufforderung, den Vorgang erneut auszuführen.***

- Prüfen Sie, ob Sie den Vorgang auf einem anderen Computer ausführen können. Ist dies der Fall, stellen Sie sicher, dass die IP-Einstellungen Ihres Computers korrekt sind (IP-Adresse, Subnetzmaske, Standardgateway und DNS). Starten Sie den Computer, bei dem das Problem aufgetreten ist, erneut.
- Falls der Computer korrekt konfiguriert ist, jedoch immer noch nicht funktioniert, überprüfen Sie das Gateway. Überprüfen Sie, ob es richtig angeschlossen und eingeschaltet ist. Stellen Sie die Verbindung mit dem Gateway her, und überprüfen Sie die Einstellungen. (Wenn Sie keine Verbindung herstellen können, prüfen Sie die LAN-Verbindung und die Stromversorgung.)
- Wenn das Gateway korrekt konfiguriert ist, prüfen Sie Ihre Internetverbindung (Kabel-/ADSL-Modem usw.), um den ordnungsgemäßen Betrieb des Gateways zu überprüfen. Sie können das Gateway entfernen, um dadurch die direkte Verbindung zu prüfen.
- Konfigurieren Sie die TCP/IP-Einstellung mithilfe einer von Ihrem ISP zur Verfügung gestellten DNS-Adresse manuell.
- Vergewissern Sie sich, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

***18. Beim Versuch, auf das webbasierte Dienstprogramm des Gateways zuzugreifen, wird der Anmeldebildschirm nicht angezeigt. Stattdessen wird die Meldung „404 Forbidden“ (404 Nicht erlaubt) angezeigt.***

Wenn Sie Internet Explorer verwenden, führen Sie die folgenden Schritte aus, bis der Anmeldebildschirm des webbasierten Dienstprogramms angezeigt wird (bei Verwendung von Netscape Navigator sind ähnliche Schritte erforderlich):

1. Klicken Sie auf **Datei**. Stellen Sie sicher, dass **Offlinebetrieb** NICHT aktiviert ist.
2. Drücken Sie die **STRG- + F5-Taste**. Dadurch wird eine Aktualisierung erzwungen und Internet Explorer veranlasst, neue und nicht gespeicherte Websites zu laden.

- Klicken Sie auf **Extras**. Klicken Sie auf **Internetoptionen**. Klicken Sie auf die Registerkarte **Sicherheit**. Klicken Sie auf die Schaltfläche **Standardstufe**. Stellen Sie sicher, dass die Sicherheitsstufe auf **Mittel** oder niedriger festgelegt ist. Klicken Sie anschließend auf die Schaltfläche **OK**.

## Häufig gestellte Fragen

***Wie viele IP-Adressen kann das Gateway maximal unterstützen?***
Das Gateway unterstützt bis zu 253 IP-Adressen.

***Unterstützt das Gateway IPSec-Passthrough?***
Ja, dabei handelt es sich um eine integrierte Funktion, die standardmäßig aktiviert ist.

***An welcher Stelle im Netzwerk wird das Gateway installiert?***
In einer typischen Umgebung wird das Gateway zwischen der ADSL-Wandbuchse und dem LAN installiert.

***Unterstützt das Gateway IPX oder AppleTalk?***
Nein. TCP/IP ist der einzige Internet-Protokollstandard und ist heutzutage globaler Kommunikationsstandard. IPX ist ein Kommunikationsprotokoll von NetWare, das nur zur Weiterleitung von Nachrichten von einem Knotenpunkt zum nächsten verwendet wird. AppleTalk ist ein Kommunikationsprotokoll, das in Apple- und Macintosh-Netzwerken für LAN-zu-LAN-Verbindungen verwendet wird. Beide Protokolle können jedoch nicht zur Verbindung des Internets mit einem LAN verwendet werden.

***Unterstützt die LAN-Verbindung des Gateways 100-Mbit/s-Ethernet?***
Das Gateway unterstützt über den EtherFast 10/100-Switch mit Auto-Sensing-Funktion auf der LAN-Seite des Gateways auch 100 Mbit/s.

***Was ist die Netzwerk-Adressen-Übersetzung, und wofür wird sie verwendet?***
Die NAT-Funktion (*Network Address Translation*; Netzwerk-Adressen-Übersetzung) übersetzt mehrere IP-Adressen in einem privaten LAN in eine öffentliche Adresse, die im Internet verwendet wird. Dadurch wird die Sicherheitsstufe erhöht, da die Adresse eines mit dem privaten LAN verbundenen Computers nie an das Internet übertragen wird. Darüber hinaus ermöglicht der Einsatz von NAT die Verwendung kostengünstiger Internetverbindungen, wenn nur eine TCP/IP-Adresse vom ISP zur Verfügung gestellt wurde. So können Benutzer mehrere private Adressen hinter einer einzigen vom ISP zur Verfügung gestellten Adresse verwenden.

***Unterstützt das Gateway auch andere Betriebssysteme als Windows 98 SE, ME, 2000 oder XP?***
Ja. Linksys bietet jedoch derzeit keinen technischen Kundendienst hinsichtlich Installation, Konfiguration oder Fehlersuche für andere Betriebssysteme als die Windows-Betriebssysteme an.

***Unterstützt das Gateway die ICQ-Dateiübertragung?***
Ja, führen Sie folgende Schritte dazu aus: Klicken Sie auf das Menü **ICQ**, **Preference** (Einstellungen) und auf die Registerkarte **Connections** (Verbindungen). Aktivieren Sie dann die Option **I am behind a firewall or proxy** (Ich bin hinter einer Firewall oder einem Proxy). Legen Sie nun in den Einstellungen für die Firewall für die Zeitüberschreitung 80 Sekunden fest. Der Internetbenutzer kann nun Dateien an Benutzer hinter dem Gateway senden.

***Ich habe einen Unreal Tournament-Server eingerichtet, andere Benutzer im LAN können sich jedoch nicht mit dem Server verbinden. Was muss ich tun?***
Nach der Installation eines dedizierten Unreal Tournament-Servers müssen Sie eine statische IP-Adresse für jeden Computer im LAN erstellen sowie die Ports 7777, 7778, 7779, 7780, 7781 und 27900 an die IP-Adresse des Servers weiterleiten. Sie können hierfür auch einen Bereich zwischen 7777 und 27900 festlegen. Um die Funktion für UT Server Admin zu verwenden, müssen Sie einen weiteren Port weiterleiten. (Das kann Port 8080 sein, der jedoch für die Remote-Verwaltung verwendet wird. Sie müssen diese Funktion u. U. deaktivieren.) Legen Sie anschließend in der Datei SERVER.INI im Abschnitt [UWeb.WebServer] für „ListenPort“ den Wert 8080 (in Übereinstimmung mit dem oben erwähnten zugeordneten Port) und für „ServerName“ die von Ihrem ISP zur Verfügung gestellte IP-Adresse des Gateways fest.

***Können mehrere Spieler im LAN auf einen Spieleserver zugreifen und mit nur einer öffentlichen IP-Adresse gleichzeitig spielen?***
Das hängt vom verwendeten Netzwerkspiel bzw. dem verwendeten Server ab. So unterstützt z. B. Unreal Tournament das mehrfache Anmelden mit nur einer öffentlichen IP-Adresse.

***Wie kann ich Half-Life - Team Fortress mit dem Gateway verwenden?***
Der standardmäßige Client-Port für Half-Life ist 27005. Für die Computer in Ihrem LAN muss in der Befehlszeile für Half-Life-Verknüpfungen „+clientport 2700x“ hinzugefügt werden, wobei „x“ dann 6, 7, 8 usw. entspricht. Dadurch können mehrere Computer mit dem gleichen Server eine Verbindung herstellen. Problem: Bei Version 1.0.1.6 können mehrere Computer, die den gleichen CD-Schlüssel verwenden, nicht gleichzeitig mit dem Server verbunden sein, auch wenn sie sich im gleichen LAN befinden. Dieses Problem tritt bei Version 1.0.1.3 nicht auf. Beim Ausführen von Spielen muss sich der Half-Life-Server jedoch nicht in der DMZ befinden. Es muss lediglich der Port 27015 an die lokale IP-Adresse des Server-Computers weitergeleitet werden.

***Die Website reagiert nicht, heruntergeladene Dateien sind beschädigt, oder es werden nur unleserliche Zeichen auf dem Bildschirm angezeigt. Was muss ich tun?***
Legen Sie für Ihren Ethernet-Adapter 10 Mbit/s bzw. den Halbduplex-Modus fest, und deaktivieren Sie als vorübergehende Maßnahme für den Ethernet-Adapter die Funktion zur automatischen Aushandlung. (Rufen Sie über die Netzwerksystemsteuerung die Registerkarte für die erweiterten Eigenschaften des Ethernet-Adapters auf.) Stellen Sie sicher, dass die Proxy-Einstellung im Browser deaktiviert ist. Weitere Informationen erhalten Sie unter www.linksys.com/international.

***Was kann ich tun, wenn alle Maßnahmen bei einer fehlgeschlagenen Installation erfolglos bleiben?***
Setzen Sie das Gateway auf die Werkseinstellungen zurück, indem Sie die Reset-Taste drücken, bis die Netzstrom-LED aufleuchtet und wieder erlischt. Setzen Sie das ADSL-Modem zurück, indem Sie es aus- und erneut einschalten. Laden Sie die neueste Firmware-Version über die internationale Website von Linksys unter www.linksys.com/international herunter, und nehmen Sie die Aktualisierung vor.

***Wie erhalte ich Informationen zu neuen Aktualisierungen der Gateway-Firmware?***
Sämtliche Aktualisierungen für Linksys-Firmware werden auf der internationalen Website von Linksys unter www.linksys.com/international veröffentlicht und können kostenlos heruntergeladen werden. Verwenden Sie zur Aktualisierung der Gateway-Firmware die Registerkarte **System** des webbasierten Dienstprogramms des Gateways. Wenn die Internetverbindung des Gateways zufriedenstellend funktioniert, besteht keine Notwendigkeit, eine neuere Firmware-Version herunterzuladen, es sei denn, Sie möchten neue Funktionen der aktualisierten Version verwenden.

***Funktioniert das Gateway in einer Macintosh-Umgebung?***
Ja, Sie können jedoch nur über Internet Explorer 4.0 bzw. Netscape Navigator 4.0 oder höher für Macintosh auf die Setup-Seiten des Gateways zugreifen.

***Ich kann die Seite für die Webkonfiguration des Gateways nicht aufrufen. Was kann ich tun?***
Sie müssen möglicherweise die Proxy-Einstellungen in Ihrem Internet-Browser, z. B. Netscape Navigator oder Internet Explorer, entfernen. Weitere Anweisungen erhalten Sie in der Dokumentation zu Ihrem Browser. Stellen Sie sicher, dass Ihr Browser die Verbindung direkt herstellt und jegliche DFÜ-Verbindung deaktiviert ist. Wenn Sie Internet Explorer verwenden, klicken Sie auf **Extras**, **Internetoptionen** und anschließend auf die Registerkarte **Verbindungen**. Stellen Sie sicher, dass für Internet Explorer die Option **Keine Verbindung wählen** aktiviert ist. Wenn Sie Netscape Navigator verwenden, klicken Sie auf **Bearbeiten**, **Einstellungen**, **Erweitert** und **Proxies**. Stellen Sie sicher, dass für Netscape Navigator die Option **Direkte Verbindung zum Internet** aktiviert ist.

***Was bedeutet DMZ-Hosting?***
Mithilfe der DMZ (*Demilitarized Zone*; Entmilitarisierte Zone) kann über eine IP-Adresse (d. h. über einen Computer) eine Verbindung zum Internet hergestellt werden. Für einige Anwendungen ist es erforderlich, dass mehrere TCP/IP-Ports geöffnet sind. Es ist empfehlenswert, dass Sie zur Verwendung des DMZ-Hostings für Ihren Computer eine statische IP-Adresse festlegen. Weitere Informationen zum Ermitteln einer LAN-IP-Adresse finden Sie in „Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters“.

***Verwenden bei DMZ-Hosting sowohl Benutzer als auch Gateway die öffentliche IP-Adresse?***
Nein.

***Leitet das Gateway PPTP-Datenpakete oder PPTP-Sitzungen aktiv weiter?***
Durch das Gateway werden PPTP-Datenpakete weitergeleitet.

***Ist das Gateway auch plattformübergreifend einsetzbar?***
Jede Plattform, die Ethernet und TCP/IP unterstützt, ist mit dem Gateway kompatibel.

***Wie viele Ports können gleichzeitig weitergeleitet werden?***
Das Gateway kann theoretisch 520 Sitzungen gleichzeitig ausführen, Sie können jedoch nur 10 Anschlussbereiche weiterleiten.

***Über welche erweiterten Funktionen verfügt das Gateway?***
Zu den erweiterten Funktionen des Gateways zählen u. a. erweiterte Wireless-Einstellungen, Filter, Port-Weiterleitung, Routing und DDNS.

***Wie viele VPN-Sitzungen unterstützt das Gateway maximal?***
Die maximale Anzahl hängt von vielen Faktoren ab. Über das Gateway wird mindestens eine IPSec-Sitzung übertragen; je nach den Spezifikationen Ihres VPNs sind jedoch auch zeitgleiche IPSec-Sitzungen möglich.

**Wie kann ich überprüfen, ob ich über statische oder DHCP-IP-Adressen verfüge?**
Wenden Sie sich an Ihren ISP, um diese Informationen zu erhalten.

***Wie kann ich mIRC mit dem Gateway verwenden?***
Legen Sie in der Registerkarte **Port Forwarding** (Port-Weiterleitung) den Wert 113 für den Computer fest, auf dem Sie mIRC verwenden möchten.

***Kann das Gateway als DHCP-Server eingesetzt werden?***
Ja. Das Gateway verfügt über eine integrierte DHCP-Server-Software.

***Kann ich Anwendungen von standortfernen Computern über das Wireless-Netzwerk ausführen?***
Dies ist abhängig davon, ob die Anwendung für die Verwendung in Netzwerken entwickelt wurde. Informationen dazu, ob die Anwendung in Netzwerken verwendet werden kann, finden Sie in der Dokumentation der entsprechenden Anwendung.

***Was ist der IEEE 802.11g-Standard?***
Dies ist ein IEEE-Standard für Wireless-Netzwerke. Mit dem 802.11g-Standard können Geräte von unterschiedlichen Herstellern im Wireless-Netzwerk miteinander kommunizieren, sofern die Geräte mit dem 802.11g-Standard kompatibel sind. Durch den 802.11g-Standard ist eine maximale Datenübertragungsrate von 54 Mbit/s und eine Betriebsfrequenz von 2,4 GHz vorgegeben.

***Welche IEEE 802.11b- und 802.11g-Funktionen werden unterstützt?***
Das Produkt unterstützt die folgenden IEEE 802.11b- und IEEE 802.11g-Funktionen:

- CSMA/CA sowie das Acknowledge-Protokoll
- Multi-Channel-Roaming
- Automatische Ratenauswahl
- RTS/CTS
- Fragmentierung
- Energieverwaltung

Es unterstützt zudem die OFDM-Technologie für 802.11g-Netzwerke.

***Was bedeutet Ad-Hoc-Modus?***
Wenn für ein Wireless-Netzwerk der Ad-Hoc-Modus festgelegt ist, sind die Wireless-Computer so konfiguriert, dass sie ohne Access Point direkt miteinander kommunizieren (Peer-to-Peer).

***Was bedeutet Infrastrukturmodus?***
Wenn für ein Wireless-Netzwerk der Infrastrukturmodus festgelegt wurde, ist es so konfiguriert, dass es über einen Wireless Access Point mit Netzwerken kommuniziert.

***Was ist Roaming?***
Roaming ermöglicht Benutzern von tragbaren Computern einen reibungslosen Datenaustausch beim Zurücklegen von Entfernungen, die nicht von einem einzigen Access Point abgedeckt werden können. Vor Verwendung des Roaming muss der Computer auf die gleiche Kanalnummer wie der Access Point des entsprechenden Empfangsbereichs gesetzt werden.

Um eine dauerhafte nahtlose Verbindung zu erzielen, muss das Wireless-LAN eine Reihe an unterschiedlichen Funktionen besitzen. So müssen z. B. alle Nachrichten von jedem Knoten und jedem Access Point bestätigt werden. Jeder Knoten muss den Kontakt mit dem Wireless-Netzwerk aufrechterhalten, auch wenn keine Datenübertragung stattfindet. Um diese Funktionen gleichzeitig verwenden zu können, ist eine dynamische Funkfrequenz-Netzwerktechnologie erforderlich, mit der Access Points und Knoten miteinander verknüpft werden. In solchen Systemen sucht der Endknoten des Benutzers nach dem jeweils besten Zugriff auf das System. Zunächst werden Faktoren wie Signalstärke und -qualität, die aktuelle Nachrichtenmenge, die von jedem Access Point verarbeitet wird, und die Entfernung zwischen jedem Access Point zum verdrahteten Backbone ausgewertet. Anschließend ermittelt der Knoten auf Grundlage dieser Informationen den geeigneten Access Point und registriert dessen Adresse. Die Kommunikation zwischen Knoten und Host-Computer kann in beide Richtungen des Backbones verlaufen.

Bei fortschreitender Kommunikation prüft der Funkfrequenz-Sender des Endknotens in regelmäßigen Abständen, ob eine Verbindung mit dem ursprünglichen Access Point vorliegt oder ob ein neuer Access Point gesucht werden soll. Wenn ein Knoten keine Bestätigung des ursprünglichen Access Point mehr erhält, wird eine neue Verbindungssuche gestartet. Wenn ein neuer Access Point gefunden wurde, wird dessen Adresse registriert und die Kommunikation fortgesetzt.

***Was bedeutet ISM-Band?***

Die FCC-Behörde und die jeweiligen Behörden außerhalb der USA haben Bestimmungen hinsichtlich der Bandbreite für eine nicht durch Lizenzen abgedeckte Verwendung im ISM-Band erlassen. Die Frequenz liegt bei ca. 2,4 GHz und kann weltweit genutzt werden. Mit dieser wahrlich revolutionären Maßnahme können nun problemlos High Speed-Wireless-Funktionen von Benutzern weltweit genutzt werden.

***Was bedeutet Bandspreizung?***

Die Technologie der Bandspreizung (*Spread Spectrum Technology*) ist eine vom Militär entwickelte Breitband-Funkfrequenz-Technologie, die für zuverlässige, sichere und störresistente Kommunikationssysteme eingesetzt werden kann. Bei dieser Technologie werden gewisse Abstriche bei der Bandbreiteneffizienz hingenommen, um eine höhere Zuverlässigkeit, Integrität und Sicherheit zu erreichen. Es wird hier also eine größere Bandbreite als bei der Schmalbandübertragung verwendet. Im Gegenzug wird jedoch ein Signal erreicht, das lauter und einfacher zu lokalisieren ist, allerdings unter der Voraussetzung, dass der Empfänger die Parameter des mittels Bandspreizung übertragenen Signals kennt. Wenn ein Empfänger nicht auf die richtige Frequenz eingestellt ist, scheint ein mittels Bandspreizung übertragenes Signal nichts anderes als ein Hintergrundgeräusch zu sein. Es stehen zwei unterschiedliche Verfahren für die Bandspreizung zur Verfügung: DSSS (*Direct Sequence Spread Spectrum*; Direkte Bandspreizung) und FHSS (*Frequency Hopping Spread Spectrum*; Frequenzsprungverfahren).

***Was ist DSSS? Was ist FHSS? Worin liegt der Unterschied?***

Bei FHSS wird ein Schmalbandträger verwendet, der nach einem für Sender und Empfänger bekannten Muster die Frequenz ändert. Bei ordnungsgemäßer Synchronisation wird jeweils ein einziger logischer Kanal aufrechterhalten. Unerwünschten Empfängern erscheint das FHSS-Signal als kurzzeitiges Impulsrauschen. DSSS generiert ein redundantes Bitmuster für jedes zu übertragende Bit. Dieses Bitmuster wird „Chip“ oder „Chipping Code“ genannt. Je länger der Chip ist, desto größer ist die Wahrscheinlichkeit, dass die ursprüngliche Information wieder generiert werden kann. Auch wenn ein oder mehrere Bits im Chip während der Übertragung beschädigt wurden, können diese durch eine statistische Technik im Empfänger regeneriert werden und müssen daher nicht nochmals übertragen werden. Unerwünschten Empfängern erscheint das DSSS-Signal als schwaches Breitbandrauschen und wird von den meisten Schmalbandempfängern ignoriert.

***Können die Daten bei der Funkübertragung abgefangen werden?***

WLAN verfügt über zweifachen Schutz im Sicherheitsbereich. Im Hardwarebereich sorgt DSSS-Technologie (*Direct Sequence Spread Spectrum*; Direkte Bandspreizung) für die integrierte Sicherheitsfunktion der Verschlüsselung. Im Softwarebereich bietet WLAN die WEP-Verschlüsselungsfunktion, um die Sicherheit zu erhöhen und die Zugriffssteuerung zu verbessern.

***Was ist WEP?***

WEP ist die Abkürzung für *Wired Equivalent Privacy*. Hierbei handelt es sich um einen Datenschutzmechanismus, der auf einem 64-Bit- oder 128-Bit-Algorithmus mit gemeinsam verwendetem Schlüssel basiert und im IEEE 802.11-Standard festgelegt ist.

***Was ist eine MAC-Adresse?***
Eine MAC-Adresse (*Media Access Control*) ist eine eindeutige Nummer, die jedem Ethernet-Netzwerkgerät, wie z. B. einem Netzwerkadapter, vom Hersteller zugewiesen wird und mit der das Gerät im Netzwerk auf Hardware-Ebene identifiziert werden kann. Aus praktischen Gründen wird diese Nummer dauerhaft vergeben. Im Gegensatz zu IP-Adressen, die sich bei jeder Anmeldung des Computers beim Netzwerk ändern können, bleibt die MAC-Adresse eines Geräts stets gleich und ist dadurch eine äußerst nützliche Kennung im Netzwerk.

***Wie setze ich das Gateway zurück?***
Halten Sie die Reset-Taste auf der Rückseite des Gateways ca. 10 Sekunden lang gedrückt. Dadurch wird das Gateway auf die Werkseinstellungen zurückgesetzt.

***Wie behebe ich einen Signalverlust?***
Sie können die genaue Reichweite Ihres Wireless-Netzwerks nur durch Testen bestimmen. Jedes Hindernis zwischen dem Gateway und einem Wireless-Computer führt zu Signalverlust. Durch verbleites Glas, Metall, Betonböden, Wasser und Wände werden Signale behindert und die Reichweite vermindert. Verwenden Sie das Gateway und den Wireless-Computer zunächst im gleichen Zimmer, und vergrößern Sie dann schrittweise den Abstand zwischen beiden Geräten, um so die maximale Reichweite in Ihrer Umgebung zu bestimmen.

Verwenden Sie auch unterschiedliche Kanäle, da so Störungen ausgeschlossen werden, die nur einen Kanal betreffen.

***Die Signalstärke ist absolut ausreichend, das Netzwerk wird jedoch nicht angezeigt.***
Die Funktion **WEP** ist vermutlich im Gateway, jedoch nicht im Wireless-Adapter (oder umgekehrt) aktiviert. Stellen Sie sicher, dass die gleichen WEP-Schlüssel und -Ebenen (64 bzw. 128) in allen Knoten in Ihrem Wireless-Netzwerk verwendet werden.

***Wie viele Kanäle/Frequenzen stehen für das Gateway zur Verfügung?***
In Nordamerika sind insgesamt 11 Kanäle, von 1 bis 11, verfügbar. Für andere Regionen stehen unter Umständen weitere Kanäle zur Verfügung. Dafür sind die Vorschriften der jeweiligen Region und/oder des jeweiligen Landes maßgebend.

Wenn Ihre Fragen hier nicht beantwortet wurden, finden Sie weitere Informationen auf der internationalen Linksys-Website unter
www.linksys.com/international.

# Anhang B: Sicherheit im Wireless-Netzwerkbetrieb

Linksys hat es sich zum Ziel gesetzt, den Wireless-Netzwerkbetrieb für Sie so sicher und einfach wie möglich zu gestalten. Die aktuellen Produkte von Linksys bieten verschiedene Netzwerksicherheitsfunktionen. Um diese anzuwenden, müssen Sie jedoch bestimmte Schritte ausführen. Beachten Sie daher Folgendes beim Einrichten bzw. Verwenden Ihres Wireless-Netzwerks.

## Vorsichtsmaßnahmen

Bei der folgenden Liste handelt es sich um eine Auflistung aller möglichen Vorsichtsmaßnahmen. Die Schritte 1 bis 5 sollten Sie unbedingt durchführen:

1. Ändern Sie die Standard-SSID.
2. Deaktivieren Sie die SSID-Übertragung.
3. Ändern Sie das Standardpasswort für das Administratorkonto.
4. Aktivieren Sie die MAC-Adressfilterung.
5. Ändern Sie die SSID regelmäßig.
6. Verwenden Sie den höchsten verfügbaren Verschlüsselungsalgorithmus. Verwenden Sie WPA (falls verfügbar). Beachten Sie, dass die Netzwerkleistung hierdurch verringert werden kann.
7. Ändern Sie die WEP-Codierschlüssel regelmäßig.

Informationen zum Umsetzen dieser Sicherheitsmaßnahmen finden Sie in „Kapitel 6: Konfigurieren des Wireless-G ADSL-Home-Gateways“.

**HINWEIS:** Einige dieser Sicherheitsfunktionen sind nur über das Netzwerk-Gateway, den Router oder den Access Point verfügbar. Weitere Informationen finden Sie in der Dokumentation zum Gateway, Router bzw. Access Point.

## Sicherheitsrisiken bei Wireless-Netzwerken

Wireless-Netzwerke sind einfach zu finden. Hacker wissen, dass Geräte für den Wireless-Netzwerkbetrieb nach so genannten Beacon-Meldungen suchen, bevor sie sich in ein Wireless-Netzwerk einklinken. Diese Meldungen, die umfassende Netzwerkinformationen wie beispielsweise die SSID (*Service Set Identifier*) des Netzwerks enthalten, lassen sich leicht entschlüsseln. Dagegen können Sie sich folgendermaßen schützen:

**Ändern Sie das Administratorpasswort regelmäßig.** Bedenken Sie, dass bei jedem im Wireless-Netzwerkbetrieb verwendeten Gerät die Netzwerkeinstellungen (SSID, WEP-Schlüssel usw.) in der Firmware gespeichert sind. Die Netzwerkeinstellungen können nur vom Netzwerkadministrator geändert werden. Wenn einem Hacker das Administratorpasswort bekannt wird, kann auch er diese Einstellungen ändern. Deshalb sollten Sie es ihm so schwer wie möglich machen, an diese Informationen zu gelangen. Ändern Sie das Administratorpasswort regelmäßig.

**SSID:** Im Zusammenhang mit der SSID ist Folgendes zu beachten:

1. Deaktivieren Sie die Übertragung.

2. Wählen Sie eine individuelle SSID.

3. Ändern Sie sie regelmäßig.

Bei den meisten Geräten für den Wireless-Netzwerkbetrieb gibt es die Option, die SSID zu übertragen. Diese Option ist zwar recht praktisch, bedeutet jedoch, dass sich jeder in Ihr Wireless-Netzwerk einklinken kann. Jeder, auch Hacker. Daher sollten Sie die SSID nicht übertragen.

Geräte für den Wireless-Netzwerkbetrieb sind werkseitig auf eine Standard-SSID eingestellt. (Die Standard-SSID von Linksys lautet „linksys“.) Hacker kennen diese Standardeinstellungen und können Ihr Netzwerk darauf überprüfen. Ändern Sie Ihre SSID, indem Sie ihr einen eindeutigen Namen zuweisen, der keinerlei Bezug zu Ihrem Unternehmen oder zu den von Ihnen verwendeten Netzwerkprodukten hat.

Ändern Sie Ihre SSID regelmäßig, damit Hacker, die sich Zugriff auf Ihr Wireless-Netzwerk verschafft haben, erneut das Passwort knacken müssen.

**MAC-Adressen:** Aktivieren Sie die MAC-Adressfilterung. Durch die MAC-Adressfilterung wird nur Wireless-Knoten mit bestimmten MAC-Adressen der Zugriff auf das Netzwerk ermöglicht. Dies erschwert es Hackern, mit einer zufällig gewählten MAC-Adresse auf Ihr Netzwerk zuzugreifen.

**WEP Encryption (WEP-Verschlüsselung).** WEP (*Wired Equivalent Privacy*) wird oft als eine Art Allheilmittel im Zusammenhang mit Sicherheitsrisiken bei Wireless-Geräten angesehen. Damit werden die Fähigkeiten von WEP jedoch überschätzt. Auch WEP kann nur soweit zur Sicherheit beitragen, dass es Hackern das Eindringen erschwert.

Es gibt mehrere Methoden, um die Wirksamkeit von WEP zu optimieren:

1. Verwenden Sie die höchste Verschlüsselungsebene.

2. Verwenden Sie die Authentifizierung mit einem freigegebenen Schlüssel.

3. Ändern Sie Ihre WEP-Schlüssel regelmäßig.

**WICHTIG:** Jedes Gerät im Wireless-Netzwerk MUSS dasselbe Verschlüsselungsverfahren und denselben Codierschlüssel verwenden, damit das Wireless-Netzwerk ordnungsgemäß funktioniert.

**WPA:** Bei **WPA** (*Wi-Fi Protected Access*) handelt es sich um den neuesten und besten verfügbaren Standard für Wi-Fi-Sicherheit. Es stehen zwei Modi zur Verfügung: **Pre-Shared Key** (Vorläufiger gemeinsamer Schlüssel) und RADIUS. Im Modus Pre-Shared Key (Vorläufiger gemeinsamer Schlüssel) stehen Ihnen zwei Verschlüsselungsverfahren zur Verfügung: **TKIP** *(Temporal Key Integrity Protocol*) und **AES** (*Advanced Encryption System*). TKIP verwendet eine leistungsfähigere Verschlüsselungsmethode sowie **MIC** (*Message Integrity Code*), um das System gegen Hacker zu schützen. AES arbeitet mit einer symmetrischen Datenverschlüsselung mit 128-Bit-Blocks. RADIUS (*Remote Authentication Dial-In User Service*) verwendet einen RADIUS-Server für die Authentifizierung sowie eine dynamische TKIP-, AES- oder WEP-Verschlüsselung.

**WPA/Pre-Shared Key** (WPA/Vorläufiger gemeinsamer Schlüssel): Wenn Sie nicht über einen RADIUS-Server verfügen, gehen Sie wie folgt vor: Wählen Sie den gewünschten Algorithmus (**TKIP** oder **AES**) aus, geben Sie im Feld **Pre-Shared Key** (Vorläufiger gemeinsamer Schlüssel) ein Passwort mit einer Länge von 8 bis 64 Zeichen ein und legen Sie für **Group Key Renewal** (Erneuerung Gruppenschlüssel) eine Zeit zwischen 0 und 99.999 Sekunden fest. Diese Zeitangabe teilt dem Gateway bzw. einem anderen Gerät mit, wie oft die Codierschlüssel auszutauschen sind.

**WPA RADIUS**: WPA wird in Verbindung mit einem RADIUS-Server verwendet. (Diese Vorgehensweise sollte nur verwendet werden, wenn ein RADIUS-Server mit einem Gateway oder einem anderen Gerät verbunden ist.) Wählen Sie zuerst den gewünschten WPA-Algorithmus aus (**TKIP** oder **AES**). Geben Sie die IP-Adresse und die Portnummer des RADIUS-Servers sowie den Schlüssel ein, der für die Verwendung durch das Gerät und den Server freigegeben ist. Legen Sie zuletzt den Zeitraum für **Group Key Renewal** (Erneuerung Gruppenschlüssel) fest. Diese Zeitangabe teilt dem Gerät mit, wie oft die Codierschlüssel auszutauschen sind.

**RADIUS**: WEP wird in Verbindung mit einem RADIUS-Server verwendet. (Diese Vorgehensweise sollte nur verwendet werden, wenn ein RADIUS-Server mit einem Gateway oder einem anderen Gerät verbunden ist.) Geben Sie zunächst die IP-Adresse und die Portnummer des RADIUS-Servers sowie den Schlüssel ein, der für die Verwendung durch das Gerät und den Server freigegeben ist. Wählen Sie dann einen WEP-Schlüssel und die WEP-Verschlüsselungsebene aus. Erzeugen Sie den WEP-Schlüssel über die Passphrase, oder geben Sie den WEP-Schlüssel manuell ein.

Die Verwendung von Verschlüsselungsfunktionen kann sich negativ auf die Netzwerkleistung auswirken. Wenn Sie jedoch sensible Daten über das Netzwerk senden, sollten Sie diese verschlüsseln.

Durch die Einhaltung dieser Sicherheitsempfehlungen können Sie ganz beruhigt arbeiten und die flexible und praktische Technologie von Linksys bedenkenlos einsetzen.

# Anhang C: Ermitteln der MAC-Adresse und der IP-Adresse des Ethernet-Adapters

In diesem Abschnitt wird beschrieben, wie Sie die MAC-Adresse für den Ethernet-Adapter Ihres Computers ermitteln, um die MAC-Filterungsfunktion des Gateways verwenden zu können. Sie können außerdem die IP-Adresse für den Ethernet-Adapter Ihres Computers ermitteln. Die IP-Adresse wird für die Filterungs-, Weiterleitungs- und DMZ-Funktionen des Gateways verwendet. Führen Sie die in diesem Anhang aufgelisteten Schritte aus, um die MAC- oder IP-Adresse des Adapters unter Windows 98, ME, 2000 bzw. XP zu ermitteln.

## Anweisungen für Windows 98/ME

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen** den Eintrag „winipcfg“ ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

2. Wählen Sie im Fenster **IP-Konfiguration** den Ethernet-Adapter aus, den Sie über ein Ethernet-Netzwerkkabel der Kategorie 5 mit dem Gateway verbunden haben. Siehe Abbildung C-1.

3. Notieren Sie die Adapteradresse so, wie sie auf dem Bildschirm des Computers angezeigt wird (siehe Abbildung C-2). Sie bildet die MAC-Adresse Ihres Ethernet-Adapters und wird im hexadezimalen Format als Folge von Zahlen und Buchstaben dargestellt.

   Die MAC-Adresse/Adapteradresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-2 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf dem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-2 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf dem Computer angezeigte Adresse kann davon abweichen.

**Hinweis:** Die MAC-Adresse wird auch als Adapteradresse bezeichnet.

**Abbildung C-1: Fenster „IP-Konfiguration“**

**Abbildung C-2: MAC-Adresse/ Adapteradresse**

## Anweisungen für Windows 2000/XP

1. Klicken Sie auf **Start** und **Ausführen**. Geben Sie im Feld **Öffnen** den Eintrag „cmd“ ein. Drücken Sie dann die Eingabetaste, oder klicken Sie auf die Schaltfläche **OK**.

**Hinweis:** Die MAC-Adresse wird auch als physikalische Adresse bezeichnet.

2. Geben Sie in die Eingabeaufforderung **„**ipconfig /all“ ein. Drücken Sie die Eingabetaste.

3. Notieren Sie die physikalische Adresse so, wie sie am Computer anzeigt wird (Abbildung C-3). Diese Adresse stellt die MAC-Adresse des Ethernet-Adapters dar. Sie wird als Folge von Zahlen und Buchstaben dargestellt.

   Die MAC-Adresse/physikalische Adresse ist der Wert, der für die MAC-Filterung verwendet wird. Bei dem Beispiel in Abbildung C-3 lautet die MAC-Adresse des Ethernet-Adapters 00-00-00-00-00-00. Die auf dem Computer angezeigte Adresse wird anders lauten.

   Bei dem Beispiel in Abbildung C-3 lautet die IP-Adresse des Ethernet-Adapters 192.168.1.100. Die auf dem Computer angezeigte Adresse kann davon abweichen.

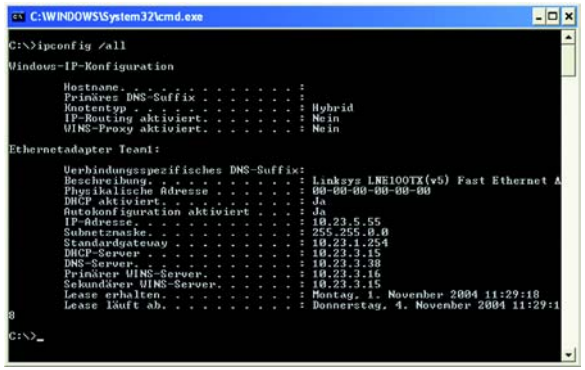

C:\WINDOWS\System32\cmd.exe
C:\>ipconfig /all
Windows-IP-Konfiguration
Hostname. . . . . :
Primäres DNS-Suffix . . . . . :
Knotentyp . . . . . : Hybrid
IP-Routing aktiviert. . . . . : Nein
WINS-Proxy aktiviert. . . . . : Nein
Ethernetadapter Team1:
Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Linksys LNE100TX(v5) Fast Ethernet A
Physikalische Adresse . . . . . : 00-00-00-00-00-00
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
IP-Adresse. . . . . : 10.23.5.55
Subnetzmaske. . . . . : 255.255.0.0
Standardgateway . . . . . : 10.23.1.254
DHCP-Server . . . . . : 10.23.3.15
DNS-Server. . . . . : 10.23.3.38
Primärer WINS-Server. . . . . : 10.23.3.16
Sekundärer WINS-Server. . . . . : 10.23.3.15
Lease erhalten. . . . . : Montag, 1. November 2004 11:29:18
Lease läuft ab. . . . . : Donnerstag, 4. November 2004 11:29:1
8
C:\>

**Abbildung C-3: MAC-Adresse/physikalische Adresse**

# Anhang D: Aktualisieren der Firmware

So aktualisieren Sie die Gateway-Firmware:

1. Laden Sie die Aktualisierungsdatei für die Gateway-Firmware von der Website *www.linksys.com* herunter.
2. Extrahieren Sie die Datei auf den Computer.
3. Öffnen Sie das webbasierte Gateway-Dienstprogramm, und klicken Sie auf die Registerkarte **Administration** (Verwaltung).
4. Klicken Sie auf die Registerkarte **Firmware Upgrade** (Firmware aktualisieren).
5. Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um nach der extrahierten Datei zu suchen, und doppelklicken Sie auf diese Datei.
6. Klicken Sie auf die Schaltfläche **Upgrade** (Aktualisieren), und befolgen Sie die Anweisungen auf dem Bildschirm.

**Abbildung D-1: Firmware aktualisieren**

# Anhang E: Glossar

**802.11b**: Ein Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 11 Mbit/s sowie eine Betriebsfrequenz von 2,4 GHz festlegt.

**802.11g**: Ein Standard für den Wireless-Netzwerkbetrieb, der eine maximale Datenübertragungsrate von 54 Mbit/s und eine Betriebsfrequenz von 2,4 GHz sowie die Abwärtskompatibilität mit Geräten festlegt, die dem Standard 802.11b entsprechen.

**Access Point**: Ein Gerät, über das Computer und andere Geräte mit Wireless-Funktionalität mit einem verdrahteten Netzwerk kommunizieren können. Wird auch verwendet, um die Reichweite von Wireless-Netzwerken zu erweitern.

**Adapter**: Ein Gerät, mit dem Ihr Computer Netzwerkfunktionalität erhalten kann.

**Ad-Hoc**: Eine Gruppe von Wireless-Geräten, die nicht über einen Access Point, sondern direkt miteinander kommunizieren (Peer-to-Peer).

**AES** (***A**dvanced **E**ncryption **S**tandard*): Eine Sicherheitsmethode, bei der die symmetrische Datenverschlüsselung mit 128-Bit-Blocks verwendet wird.

**Aktualisierung**: Das Ersetzen vorhandener Software oder Firmware durch eine neuere Version.

**Backbone**: Der Teil des Netzwerks, der die meisten Systeme und Netzwerke miteinander verbindet und die meisten Daten verarbeitet.

**Bandbreite**: Die Übertragungskapazität eines bestimmten Geräts oder Netzwerks.

**Bandspreizung**: Weitband-Funkfrequenzmethode, die für eine zuverlässigere und sicherere Datenübertragung verwendet wird.

**Beacon-Intervall**: Im Wireless-Netzwerk übertragene Daten zur Synchronisierung des Netzwerks.

**Bit**: Eine binäre Einheit.

**Breitband**: Eine stets aktive, schnelle Internetverbindung.

**Bridge**: Ein Gerät, das verschiedene Netzwerke miteinander verbindet.

**Browser**: Eine Anwendung, mit der auf alle im World Wide Web enthaltenen Informationen interaktiv zugegriffen werden kann.

**Byte**: Eine Dateneinheit, die üblicherweise aus acht Bits besteht.

**CSMA/CA** (***C****arrier* ***S****ense* ***M****ultiple* ***A****ccess/****C****ollision* ***A****voidance*): Eine Datenübertragungsmethode, die verwendet wird, um Datenkollisionen zu verhindern.

**CTS** (***C****lear* ***T****o* ***S****end*): Ein von einem Wireless-Gerät gesendetes Signal, das angibt, dass das Gerät für Daten empfangsbereit ist.

**Daisy Chain** (Verkettung): Eine Methode, bei der Geräte in Reihe (in einer Kette) miteinander verbunden werden.

**Datenbank**: Eine Datensammlung, die so organisiert ist, dass die enthaltenen Daten schnell und einfach verwaltet und aktualisiert werden können sowie problemlos abrufbar sind.

**DDNS** (***D****ynamic* ***D****omain* ***N****ame* ***S****ystem*): Ermöglicht das Hosten von Websiten, FTP-Servern oder E-Mail-Servern mit festen Domänennamen (z. B. www.xyz.com) und dynamischen IP-Adressen.

**DHCP** (***D****ynamic* ***H****ost* ***C****onfiguration* ***P****rotocol*): Ein Netzwerkprotokoll, mit dem Administratoren Netzwerkcomputern temporäre IP-Adressen zuweisen können, indem sie IP-Adressen für einen bestimmten Zeitraum an Benutzer „vermieten“ statt ihnen eine permanente IP-Adresse zuzuweisen.

**DMZ** (***De****militarized* ***Z****one*): Hebt den Firewall-Schutz des Routers für einen PC auf, so dass dieser im Internet „sichtbar“ wird.

**DNS** (***D****omain* ***N****ame* ***S****erver*): Die IP-Adresse des Servers Ihres Internetdienstanbieters, der die Namen von Websites in IP-Adressen übersetzt.

**Domäne**: Ein spezifischer Name für ein Netzwerk aus mehreren Computern.

**DSL** (***D****igital* ***S****ubscriber* ***L****ine*): Eine stets aktive Breitbandverbindung über herkömmliche Telefonleitungen.

**DSSS** (***D****irect-****S****equence* ***S****pread-****S****pectrum*): Eine Frequenzübertragungstechnologie, die ein redundantes Bit-Muster verwendet, um die Wahrscheinlichkeit von Datenverlusten bei der Übertragung zu senken.

**DTIM** (***D****elivery* ***T****raffic* ***I****ndication* ***M****essage*): Eine in Datenpaketen enthaltene Nachricht, die zur Verbesserung der Effizienz von Wireless-Verbindungen beitragen kann.

**Durchsatz**: Die Datenmenge, die in einem bestimmten Zeitraum erfolgreich von einem Knoten an einen anderen übertragen werden kann.

**Dynamische IP-Adresse**: Eine von einem DHCP-Server zugewiesene temporäre IP-Adresse.

**EAP** (***E**xtensible **A**uthentication **P**rotocol*): Ein allgemeines Authentifizierungsprotokoll zur Steuerung des Netzwerkzugriffs. Viele spezielle Authentifizierungsmethoden greifen auf dieses Protokoll zurück.

**EAP-PEAP** (***E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifzierungsmethode, bei der eine Kombination aus digitalen Zertifikaten und einem anderen System, z. B. Passwörter, verwendet wird.

**EAP-TLS** (***E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity*): Eine gegenseitige Authentifizierungsmethode, bei der digitale Zertifikate verwendet werden.

**Ethernet**: Ein Netzwerkprotokoll, mit dem festgelegt wird, wie Daten auf gängigen Übertragungsmedien gespeichert und von dort abgerufen werden.

**Finger**: Ein Programm, das Ihnen den Namen angibt, der einer E-Mail-Adresse zugewiesen ist.

**Firewall**: Eine Gruppe von Programmen, die sich auf einem Netzwerk-Gateway-Server befindet und die Ressourcen des Netzwerks vor unberechtigten Benutzern schützt.

**Firmware**: Der für ein Netzwerkgerät verwendete Programmiercode.

**Fragmentierung**: Das Aufteilen von Paketen in kleinere Einheiten bei der Übertragung über Netzwerkmedien, die die ursprüngliche Größe des Pakets nicht unterstützen.

**FTP** (***F**ile **T**ransfer **P**rotocol*): Ein Protokoll für die Übertragung von Dateien über ein TCP/IP-Netzwerk.

**Gateway**: Ein Gerät zur Verbindung von Netzwerken mit unterschiedlichen, inkompatiblen Kommunikationsprotokollen.

**Halbduplex**: Datenübertragung, die über eine Leitung in beide Richtungen erfolgt, jedoch entweder in die eine oder die andere Richtung, nicht gleichzeitig in beide.

**Hardware**: Als Hardware bezeichnet man die physischen Geräte im Computer- und Telekommunikationsbereich sowie andere Informationstechnologiegeräte.

**Herunterladen**: Das Empfangen einer Datei, die über ein Netzwerk übertragen wurde.

**Hochfahren**: Starten von Geräten, so dass diese Befehle ausführen.

**HTTP** (***H**yper**T**ext **T**ransport **P**rotocol*): Kommunikationsprotokoll, mit dem Verbindungen zu Servern im World Wide Web hergestellt werden.

**Infrastruktur**: Ein Wireless-Netzwerk, das über einen Access Point mit einem verdrahteten Netzwerk verbunden ist.

**IP** (***I****nternet* ***P****rotocol*): Ein Protokoll zum Senden von Daten über Netzwerke.

**IP-Adresse**: Die Adresse, anhand der ein Computer oder ein Gerät im Netzwerk identifiziert werden kann.

**IPCONFIG**: Ein Dienstprogramm für Windows 2000 und Windows XP, das die IP-Adresse von bestimmten Geräten im Netzwerk anzeigt.

**IPSec** (***I****nternet* ***P****rotocol* ***Sec****urity*): Ein VPN-Protokoll, das für den sicheren Austausch von Paketen auf der IP-Ebene verwendet wird.

**ISM-Band**: Bei Übertragungen im Wireless-Netzwerkbetrieb verwendete Funkbandbreite.

**ISP** (***I****nternet* ***S****ervice* ***P****rovider*): Internetdienstanbieter; ein Anbieter, über den auf das Internet zugegriffen werden kann.

**Kabelmodem**: Ein Gerät, über das ein Computer mit dem Kabelfernsehnetzwerk verbunden wird, das wiederum eine Verbindung zum Internet herstellt.

**Knoten**: Ein Netzwerkknotenpunkt bzw. -verbindungspunkt, üblicherweise ein Computer oder eine Arbeitsstation.

**Laden**: Das Übertragen einer Datei über das Netzwerk.

**LAN**: Die Computer und Netzwerkprodukte, aus denen sich Ihr lokales Netzwerk zusammensetzt.

**LEAP** (***L****ightweight* ***E****xtensible* ***A****uthentication* ***P****rotocol*): Eine gegenseitige Authentifizierungsmethode, bei der ein Benutzername- und Passwortsystem verwendet wird.

**MAC-Adresse** (***M****edia* ***A****ccess* ***C****ontrol*)**:** Die eindeutige Adresse, die ein Hersteller jedem einzelnen Netzwerkbetriebsgerät zuweist.

**Mbit/s** (***M****ega****bit*** *pro* ***S****ekunde*): Eine Million Bit pro Sekunde. Maßeinheit für die Datenübertragung.

**mIRC**: Ein unter Windows verwendetes Internet Relay Chat-Programm.

**Multicasting**: Das gleichzeitige Senden von Daten an mehrere Ziele.

**NAT** (***N****etwork* ***A****ddress* ***T****ranslation*): Die NAT-Technologie übersetzt IP-Adressen von lokalen Netzwerken in eine andere IP-Adresse für das Internet.

**Netzwerk**: Mehrere Computer oder Geräte, die miteinander verbunden sind, damit Benutzer Daten gemeinsam verwenden, speichern und untereinander übertragen können.

**NNTP** (***N**etwork **N**ews **T**ransfer **P**rotocol*): Das Protokoll, mit dem eine Verbindung zu Usenet-Gruppen im Internet hergestellt wird.

**OFDM** (***O**rthogonal **F**requency **D**ivision **M**ultiplexing*): Eine Frequenzübertragungstechnologie, die den Datenstrom in mehrere Datenströme von geringerer Geschwindigkeit aufteilt, die dann parallel übertragen werden, um zu verhindern, dass Informationen während der Übertragung verloren gehen.

**Paket**: Eine Dateneinheit, die über Netzwerke gesendet wird.

**Passphrase**: Wird wie ein Passwort verwendet und erleichtert die WEP-Verschlüsselung, indem für Linksys Produkte automatisch WEP-Codierschlüssel erstellt werden.

**PEAP** (***P**rotected **E**xtensible **A**uthentication **P**rotocol*): Eine gegenseitige Authentifzierungsmethode, bei der eine Kombination aus digitalen Zertifikaten und einem anderen System, z. B. Passwörter, verwendet wird.

**Ping** (***P**acket **IN**ternet **G**roper*): Ein Internetdienstprogramm, mit dem bestimmt werden kann, ob eine bestimmte IP-Adresse online ist.

**POP3** (***P**ost **O**ffice **P**rotocol **3***): Ein im Internet verwendeter Standard-Mail-Server.

**Port**: Der Anschlusspunkt an einem Computer oder Netzwerkbetriebsgerät, an den Kabel oder Adapter angeschlossen werden.

**P**ower **o**ver **E**thernet (***PoE***): Eine Technologie, mit der über Ethernet-Netzwerkkabel sowohl Daten als auch Strom übertragen werden kann.

**PPPoE** (***P**oint to **P**oint **P**rotocol **o**ver **E**thernet*): Eine Art der Breitbandverbindung, die neben der Datenübertragung eine Authentifizierungsmöglichkeit (Benutzername und Passwort) bietet.

**PPTP** (***P**oint-to-**P**oint **T**unneling **P**rotocol*): Ein VPN-Protokoll, mit dem das Point-to-Point-Protokoll (PPP) über einen Tunnel durch das IP-Netzwerk geleitet werden kann. Dieses Protokoll wird darüber hinaus in Europa als eine Art der Breitbandverbindung verwendet.

**Präambel**: Teil des Wireless-Signals, mit dem der Netzwerkdatenverkehr synchronisiert wird.

**Puffer**: Puffer sind freigegebene oder zugewiesene Speicherbereiche zur Unterstützung und Koordinierung von verschiedenen Computer- und Netzwerkaktivitäten, damit sich diese nicht gegenseitig behindern oder aufhalten.

**RADIUS** (***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*): Ein Protokoll zur Überwachung des Netzwerkzugriffs mithilfe eines Authentifizierungsservers.

**RJ-45** (**R**egistered **J**ack**-45**): Ethernet-Anschluss für bis zu acht Drähte.

**Roaming**: Die Möglichkeit, mit einem Wireless-Gerät aus einem Access Point-Bereich in einen anderen zu wechseln, ohne die Verbindung zu unterbrechen.

**Router**: Ein Netzwerkgerät, mit dem mehrere Netzwerke miteinander verbunden werden.

**RTS** (*Request To Send*): Eine Methode zur Koordination von großen Datenpaketen in einem Netzwerk mithilfe der RTS-Schwelle.

**Server**: Ein beliebiger Computer, der innerhalb eines Netzwerks dafür sorgt, dass Benutzer auf Dateien zugreifen, kommunizieren sowie Druckvorgänge und andere Aktionen ausführen können.

**SMTP** (***S**imple **M**ail **T**ransfer **P**rotocol*): Das standardmäßige E-Mail-Protokoll im Internet.

**SNMP** (***S**imple **N**etwork **M**anagement **P**rotocol*): Ein weit verbreitetes und häufig verwendetes Protokoll zur Netzwerküberwachung und -steuerung.

**Software**: Befehle für den Computer. Eine Folge von Befehlen, mit denen eine bestimmte Aufgabe ausgeführt wird, wird als „Programm“ bezeichnet.

**SOHO** (***S**mall **O**ffice/**H**ome **O**ffice*): Marktsegment der Geschäftkunden, die zu Hause oder in kleineren Büros arbeiten.

**SPI-Firewall** (***S**tateful **P**acket **I**nspection*): Eine Technologie, mit der eingehende Datenpakete vor der Weiterleitung an das Netzwerk überprüft werden.

**SSID** (***S**ervice **S**et **ID**entifier*): Der Name Ihres Wireless-Netzwerks.

**Standard-Gateway**: Ein Gerät, über das der Internetdatenverkehr Ihres LANs weitergeleitet wird.

**Statische IP-Adresse**: Eine feste Adresse, die einem in ein Netzwerk eingebundenen Computer oder Gerät zugewiesen ist.

**Statisches Routing**: Das Weiterleiten von Daten in einem Netzwerk über einen festen Pfad.

**Subnetzmaske**: Ein Adressencode, der die Größe des Netzwerks festlegt.

**Switch**: 1. Ein Daten-Switch, der Rechner mit Host-Computern verbindet, wodurch eine begrenzte Anzahl von Ports von mehreren Geräten gemeinsam genutzt werden kann. 2. Ein Gerät zum Herstellen, Trennen und Ändern der Verbindungen innerhalb von elektrischen Schaltkreisen.

**TCP** (***T**ransmission **C**ontrol **P**rotocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem eine Bestätigung des Empfängers der gesendeten Daten erforderlich ist.

**TCP/IP** (***T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol*): Ein Satz von Anweisungen, den alle PCs für die Kommunikation über Netzwerke verwenden.

**Telnet**: Benutzerbefehl und TCP/IP-Protokoll zum Zugriff auf entfernte PCs.

**TFTP** (***T**rivial **F**ile **T**ransfer **P**rotocol*): Eine Version des TCP/IP-FTP-Protokolls, das über keinerlei Verzeichnis- oder Passwortfunktionalitäten verfügt.

**TKIP** (***T**emporal **K**ey **I**ntegrity **P**rotocol*): Eine Wireless-Verschlüsselungsmethode, bei der für jedes übertragene Datenpaket dynamische Codierschlüssel zur Verfügung stehen.

**Topologie**: Die physische Anordnung eines Netzwerks.

**TX-Rate**: Übertragungsrate.

**UDP** (***U**ser **D**atagram **P**rotocol*): Ein Netzwerkprotokoll zur Datenübertragung, bei dem keine Bestätigung vom Empfänger der gesendeten Daten erforderlich ist.

**URL** (***U**niform **R**esource **L**ocator*): Die Adresse einer im Internet befindlichen Datei.

**Verschlüsselung**: Die Codierung von Daten, die über Netzwerke übertragen werden.

**Vollduplex**: Die Fähigkeit von Netzwerkgeräten, Daten gleichzeitig empfangen und übertragen zu können.

**VPN** (***V**irtual **P**rivate **N**etwork*): Eine Sicherheitsmaßnahme, mit der Daten geschützt werden, wenn sie über das Internet von einem Netzwerk in ein anderes übertragen werden.

**WAN** (***W**ide **A**rea **N**etwork*): Das Internet.

**WEP** (***W**ired **E**quivalent **P**rivacy*): Eine hochgradig sichere Methode zum Verschlüsseln von Netzwerkdaten, die in Wireless-Netzwerken übertragen werden.

**WINIPCFG**: Ein Dienstprogramm für Windows 98 und Windows ME, das die IP-Adresse bestimmter Netzwerkbetriebsgeräte anzeigt.

**WLAN** (*Wireless Local Area Network*): Eine Reihe von Computern und Geräten, die über Funkverbindungen miteinander kommunizieren.

**WPA** (*Wi-Fi Protected Access*): Ein Wireless-Sicherheitsprotokoll, bei dem eine TKIP-Verschlüsselung (*Temporal Key Integrity Protocol*) verwendet wird, die zusammen mit einem RADIUS-Server eingesetzt werden kann

# Anhang F: Zulassungsinformationen

FCC-Bestimmungen

Dieses Gerät wurde geprüft und entspricht den Bestimmungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Die Grenzwerte wurden so festgelegt, dass ein angemessener Schutz gegen Störungen in einer Wohngegend gewährleistet ist. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und kann diese abstrahlen. Wird es nicht gemäß den Angaben des Herstellers installiert und betrieben, kann es sich störend auf den Rundfunk- und Fernsehempfang auswirken. Es besteht jedoch keine Gewähr, dass bei einer bestimmten Installation keine Störungen auftreten. Sollte dieses Gerät Störungen des Radio- und Fernsehempfangs verursachen (was durch Ein- und Ausschalten des Geräts feststellbar ist), wird der Benutzer aufgefordert, die Störungen durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus, oder stellen Sie sie an einem anderen Ort auf.
- Erhöhen Sie den Abstand zwischen der Ausrüstung oder den Geräten.
- Schließen Sie das Gerät an eine anderen Anschluss als den des Empfängers an.
- Wenden Sie sich bei Fragen an Ihren Händler oder an einen erfahrenen Funk-/Fernsehtechniker.

FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung

Dieses Gerät erfüllt die FCC-Bestimmungen zur Freisetzung gefährlicher Strahlung in einer nicht gesteuerten Umgebung. Dieses Gerät sollte so installiert und betrieben werden, dass der Abstand zwischen dem Radiator und Personen mindestens 20 cm beträgt.

Kanadische Industriebestimmungen

Dieses Gerät erfüllt die kanadischen Bestimmungen der Richtlinien ICES-003 und RSS210.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry Canada.

Informationen zur Einhaltung gesetzlicher Vorschriften bei 2,4-GHz-Wireless-Produkten für den Bereich der EU und anderer Länder gemäß der EU-Richtlinie 1999/5/EG (R&TTE-Richtlinie)

Konformitätserklärung zur EU-Richtlinie 1995/5/EG (R&TTE-Richtlinie)

| | |
|---|---|
| Česky [Czech]: | Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC. |
| Dansk [Danish]: | Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF. |
| Deutsch [German]: | Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU. |
| Eesti [Estonian]: | See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele. |
| English: | This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. |
| Español [Spanish]: | Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE. |
| Ελληνική [Greek]: | Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/ΕC. |
| Français [French]: | Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC. |
| Íslenska [Icelandic]: | Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC. |
| Italiano [Italian]: | Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE. |
| Latviski [Latvian]: | Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. |
| Lietuvių [Lithuanian]: | Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas. |
| Nederlands [Dutch]: | Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC. |
| Malti [Maltese]: | Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC. |
| Margyar [Hungarian]: | Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket. |

| | |
|---|---|
| Norsk [Norwegian]: | Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF. |
| Polski [Polish]: | Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC. |
| Português [Portuguese]: | Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC. |
| Slovensko [Slovenian]: | Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC. |
| Slovensky [Slovak]: | Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC. |
| Suomi [Finnish]: | Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen. |
| Svenska [Swedish]: | Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC. |

**Hinweise:** Die vollständige Konformitätserklärung finden Sie entweder auf der CD oder in einem separaten Dokument, das diesem Produkt beigefügt ist.

Wenn Sie weitere technische Dokumente benötigen, finden Sie diesbezügliche Informationen unter „Technische Dokumente unter www.linksys.com/international“ weiter hinten in diesem Anhang.

Bei der Bewertung des Produkts hinsichtlich der Anforderung der Richtlinie 1999/5/EG kamen die folgenden Standards zur Anwendung:

- Funkausrüstung: EN 300 328
- EMV: EN 301 489-1, EN 301 489-17
- Sicherheit: EN 60950

CE-Kennzeichnung

Die Wireless-B- und Wireless-G-Produkte von Linksys sind mit der folgenden CE-Kennzeichnung, der Nummer der Überwachungs- und Zertifizierungsstelle (sofern zutreffend) und der Kennung der Klasse 2 versehen.

CE 0560 ① oder CE 0678 ① oder CE ①

Überprüfen Sie das CE-Etikett auf dem Produkt, um die Überwachungs- und Zertifizierungsstelle zu ermitteln, die in die Bewertung einbezogen wurde.

Nationale Beschränkungen

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

*Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:*

*Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:*

*Das Produkt kann in allen EU-Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten, die der EU-Richtlinie 1999/5/EG folgen), mit Ausnahme der folgenden Staaten:*

Belgien

Wireless-Verbindungen im Freien mit einer Reichweite über 300 m müssen beim Belgischen Institut für Postdienste und Telekommunikation (BIPT) angemeldet werden. Weitere Informationen finden Sie unter http://www.bipt.be.

*Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.*

*Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT).*
*Visitez http://www.ibpt.be pour de plus amples détails.*

Frankreich

Bei Verwendung des Produkts im Freien gelten für die Ausgangsleistung in bestimmten Bandbereichen Beschränkungen. Weitere Informationen finden Sie in Tabelle 1 oder unter http://www.art-telecom.fr/.

*Dans la cas d'une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous à la table 1 ou visitez http://www.art-telecom.fr/ pour de plus amples détails.*

Tabelle 1: In Frankreich zulässige Leistungspegel

| **Standort** | **Frequenzbereich (MHz)** | **Leistung (EIRP; *Effective Isotropic Radiated Power*)** |
|---|---|---|
| In Gebäuden (keine Beschränkungen) | 2400-2483,5 | 100 mW (20 dBm) |
| Im Freien | 2400-2454<br>2454-2483,5 | 100 mW (20 dBm)<br>10 mW (10 dBm) |

Italien

Dieses Produkt entspricht den nationalen Vorschriften für Funkschnittstellen und den in der nationalen Frequenzzuweisungstabelle für Italien aufgeführten Anforderungen. Für den Betrieb dieses 2,4-GHz-Wireless-LAN-Produkts außerhalb der Grundstücksgrenzen des Eigentümers ist eine allgemeine Genehmigung erforderlich. Weitere Informationen finden Sie unter http://www.comunicazioni.it/it/.

*Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.*

Beschränkungen hinsichtlich der Verwendung des Produkts

Dieses Produkt wurde ausschließlich für die Verwendung in Gebäuden entwickelt. Die Verwendung im Freien wird nicht empfohlen.

Dieses Produkt wurde für die Verwendung mit der im Lieferumfang enthaltenen standardmäßigen, integrierten bzw. externen (speziell für diesen Zweck vorgesehenen) Antenne entwickelt. Manche Anwendungen setzen jedoch unter Umständen voraus, dass Sie die Antenne(n) vom Produkt trennen und mithilfe eines Verlängerungskabels an einem anderen Ort als das Gerät installieren. Für diese Anwendungen bietet Linksys ein R-SMA-Verlängerungskabel (AC9SMA) und ein R-TNC-Verlängerungskabel (AC9TNC). Beide Kabel sind neun Meter lang. Der Verlust durch das Kabel (die Abschwächung) liegt bei 5 dB. Zur Kompensation der Abschwächung bietet Linksys außerdem die Hochleistungsantennen HGA7S (mit R-SMA-Stecker) und HGA7T (mit R-TNC-Stecker). Diese Antennen verfügen über einen Antennengewinn von 7 dBi und dürfen nur mit dem R-SMA- oder R-TNC-Verlängerungskabel eingesetzt werden.

Kombinationen von Verlängerungskabeln und Antennen, die zu einem ausgestrahlten Leistungspegel von mehr als 100 mW EIRP (*Effective Isotropic Radiated Power*) führen, sind unzulässig.

Ausgangsleistung des Geräts

Zur Einhaltung der jeweiligen nationalen Vorschriften müssen Sie u. U. die Ausgangsleistung Ihres Wireless-Geräts anpassen. Fahren Sie mit dem entsprechenden Abschnitt für Ihr Gerät fort.

**Hinweise:** Die Einstellungen für die Ausgangsleistung sind u. U. nicht für alle Wireless-Produkte verfügbar. Weitere Informationen finden Sie in der Dokumentation auf der Produkt-CD oder unter http://www.linksys.com/international.

Wireless-Adapter

Bei Wireless-Adaptern ist die Ausgangsleistung standardmäßig auf 100 % eingestellt. Die Ausgangsleistung der einzelnen Adapter beträgt maximal 20 dBm (100 mW), liegt aber gewöhnlich bei 18 dBm (64 mW) oder darunter. Wenn Sie die Ausgangsleistung Ihres Wireless-Adapters anpassen müssen, befolgen Sie die entsprechenden Anweisungen für das Windows-Betriebssystem Ihres Computers:

Windows XP

1. Doppelklicken Sie auf dem Desktop in der Taskleiste auf das Symbol **Drahtlose Verbindung**.
2. Öffnen Sie das Fenster *Drahtlose Netzwerkverbindung*.
3. Klicken Sie auf die Schaltfläche **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Allgemein** und dann auf die Schaltfläche **Konfigurieren**.
5. Klicken Sie im Fenster *Eigenschaften* auf die Registerkarte **Erweitert**.
6. Wählen Sie **Ausgangsleistung** aus.
7. Wählen Sie aus dem rechts angezeigten Pulldown-Menü den Prozentsatz für die Ausgangsleistung des Wireless-Adapters aus.

Windows 2000

1. Öffnen Sie das Fenster **Systemsteuerung**.
2. Doppelklicken Sie auf **Netzwerk- und DFÜ-Verbindungen**.
3. Wählen Sie Ihre aktuelle Wireless-Verbindung aus, und wählen Sie dann **Eigenschaften**.
4. Klicken Sie im Fenster *Eigenschaften* auf die Schaltfläche **Konfigurieren**.
5. Klicken Sie auf die Registerkarte **Erweitert**, und wählen Sie **Ausgangsleistung** aus.
6. Wählen Sie aus dem rechts angezeigten Pulldown-Menü die Leistungseinstellung für den Wireless-Adapter aus.

Wenn auf Ihrem Computer Windows ME oder Windows 98 ausgeführt wird, finden Sie in der Windows-Hilfe Anweisungen zum Aufrufen der erweiterten Einstellungen von Netzwerkadaptern.

Wireless Access Points, Router und andere Wireless-Produkte

Wenn Sie über einen Wireless Access Point, einen Router oder ein anderes Wireless-Produkt verfügen, verwenden Sie das zugehörige webbasierte Dienstprogramm, um die Einstellungen für die Ausgangsleistung zu konfigurieren (weitere Informationen finden Sie in der Dokumentation zum jeweiligen Produkt).

## Technische Dokumente unter www.linksys.com/international

Führen Sie die folgenden Schritte aus, um auf die gewünschten technischen Dokumente zuzugreifen:

1. Navigieren Sie mit dem Browser zur Website http://www.linksys.com/international.
2. Klicken Sie auf Ihre Region.
3. Klicken Sie auf den Namen Ihres Landes.
4. Klicken Sie auf **Produkt**.
5. Klicken Sie auf die entsprechende Produktkategorie.
6. Wählen Sie ein Produkt aus.
7. Klicken Sie auf den gewünschten Dokumentationstyp. Das Dokument wird automatisch im PDF-Format geöffnet.

**Hinweise:** Wenn Sie Fragen zur Einhaltung gesetzlicher Vorschriften in Bezug auf diese Produkte haben oder die gewünschten Informationen nicht finden können, wenden Sie sich an die Vertriebsniederlassung vor Ort, oder rufen Sie weitere Einzelheiten unter http://www.linksys.com/international ab.

# Anhang G: Garantieinformationen

Linksys sichert Ihnen für einen Zeitraum von drei Jahren (die „Gewährleistungsfrist“) zu, dass dieses Linksys Produkt bei normaler Verwendung keine Material- oder Verarbeitungsfehler aufweist. Im Rahmen dieser Gewährleistung beschränken sich Ihre Rechtsmittel und der Haftungsumfang von Linksys wie folgt: Linksys kann nach eigenem Ermessen das Produkt reparieren oder austauschen oder Ihnen den Kaufpreis abzüglich etwaiger Nachlässe zurückerstatten. Diese eingeschränkte Gewährleistung gilt nur für den ursprünglichen Käufer.

Sollte sich das Produkt während der Gewährleistungsfrist als fehlerhaft erweisen, wenden Sie sich an den technischen Kundendienst von Linksys, um eine so genannte *Return Authorization Number* (Nummer zur berechtigten Rücksendung) zu erhalten. WENN SIE SICH AN DEN TECHNISCHEN KUNDENDIENST WENDEN, SOLLTEN SIE IHREN KAUFBELEG ZUR HAND HABEN. Wenn Sie gebeten werden, das Produkt einzuschicken, geben Sie die Nummer zur berechtigten Rücksendung gut sichtbar auf der Verpackung an und legen Sie eine Kopie des Originalkaufbelegs bei. RÜCKSENDEANFRAGEN KÖNNEN NICHT OHNE DEN KAUFBELEG BEARBEITET WERDEN. Der Versand fehlerhafter Produkte an Linksys erfolgt auf Ihre Verantwortung. Linksys kommt nur für Versandkosten von Linksys zu Ihrem Standort per UPS auf dem Landweg auf. Bei Kunden außerhalb der USA und Kanadas sind sämtliche Versand- und Abfertigungskosten durch die Kunden selbst zu tragen.

ALLE GEWÄHRLEISTUNGEN UND BEDINGUNGEN STILLSCHWEIGENDER ART HINSICHTLICH DER MARKTÜBLICHEN QUALITÄT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK SIND AUF DIE DAUER DER GEWÄHRLEISTUNGSFRIST BESCHRÄNKT. JEGLICHE WEITEREN BEDINGUNGEN, ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN SOWOHL AUSDRÜCKLICHER ALS AUCH STILLSCHWEIGENDER ART, EINSCHLIESSLICH JEGLICHER STILLSCHWEIGENDER GEWÄHRLEISTUNG DER NICHTVERLETZUNG, WERDEN AUSGESCHLOSSEN. Einige Gerichtsbarkeiten gestatten keine Beschränkungen hinsichtlich der Gültigkeitsdauer einer stillschweigenden Gewährleistung; die oben genannte Beschränkung findet daher unter Umständen auf Sie keine Anwendung. Die vorliegende Gewährleistung sichert Ihnen bestimmte gesetzlich verankerte Rechte zu. Darüber hinaus stehen Ihnen je nach Gerichtsbarkeit unter Umständen weitere Rechte zu.

Diese Gewährleistung gilt nicht, wenn das Produkt (a) von einer anderen Partei als Linksys verändert wurde, (b) nicht gemäß den von Linksys bereitgestellten Anweisungen installiert, betrieben, repariert oder gewartet wurde oder (c) unüblichen physischen oder elektrischen Belastungen, Missbrauch, Nachlässigkeit oder Unfällen ausgesetzt wurde. Darüber hinaus kann Linksys angesichts der ständigen Weiterentwicklung neuer Methoden zum unerlaubten Zugriff und Angriff auf Netzwerke nicht gewährleisten, dass das Produkt keinerlei Schwachstellen für unerlaubte Zugriffe oder Angriffe bietet.

SOWEIT NICHT GESETZLICH UNTERSAGT, SCHLIESST LINKSYS JEGLICHE HAFTUNG FÜR VERLOREN GEGANGENE DATEN, ENTGANGENE EINNAHMEN, ENTGANGENE GEWINNE ODER SONSTIGE SCHÄDEN BESONDERER, INDIREKTER, MITTELBARER, ZUFÄLLIGER ODER BESTRAFENDER ART AUS, DIE SICH AUS DER VERWENDUNG BZW. DER NICHTVERWENDBARKEIT DES PRODUKTS (AUCH DER SOFTWARE) ERGEBEN ODER MIT DIESER ZUSAMMENHÄNGEN, UNABHÄNGIG VON DER HAFTUNGSTHEORIE (EINSCHLIESSLICH NACHLÄSSIGKEIT), AUCH WENN LINKSYS ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. DIE HAFTUNG VON LINKSYS IST STETS AUF DEN FÜR DAS PRODUKT GEZAHLTEN BETRAG BESCHRÄNKT. Die oben genannten Beschränkungen kommen auch dann zur Anwendung, wenn eine in diesem Abschnitt aufgeführte Gewährleistung oder Zusicherung ihren wesentlichen Zweck verfehlt. Einige Gerichtsbarkeiten gestatten keinen Ausschluss von bzw. keine Beschränkungen auf zufällige oder Folgeschäden; die oben genannte Beschränkung oder der oben genannte Ausschluss findet daher unter Umständen auf Sie keine Anwendung.

**Die vorliegende Gewährleistung ist nur in dem Land gültig bzw. kann nur in dem Land verarbeitet werden, in dem das Produkt erworben wurde.**

Richten Sie alle Anfragen direkt an: Linksys, P.O. Box 18558, Irvine, CA 92623, USA.

# Anhang H: Spezifikationen

| | |
|---|---|
| Modellnummer | WAG354G |
| Standards | IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, G.992.1 (G.dmt), G.992.2 (G.lite), G.992.3, G.992.5, T1.413i2 |
| Ports | Netzstrom, ADSL, Ethernet (1-4) |
| Taste | Eine Reset-Taste |
| Kabeltyp | Kat. 5 UTP |
| LEDs | Netzstrom, Wireless, Ethernet (1-4), DSL, Internet |
| Anzahl Antennen | 1 |
| Art der Steckverbindung | SMA |
| Abnehmbar (j/n) | Ja |
| Antennengewinn in dBi | 2 dBi |
| Übertragungsleistung | 18 dBm |
| Kanäle | 13 (in den meisten Teilen Europas) |
| UPnP-fähig/-zertifiziert | UPnP-fähig |
| Sicherheitsmerkmale | Passwortgeschützte Konfiguration für Web-Zugriff<br>PAP- und CHAP-Authentifizierung<br>DoS-Schutz (Denial of Service)<br>URL-Filterung sowie Blockieren von Stichwörtern, Java, ActiveX, Proxy und Cookies |

| | |
|---|---|
| | ToD-Filter (Blockieren des Zugriffs nach Zeit)<br>VPN-Passthrough für IPSec-, PPTP- und L2TP-Protokolle<br>WEP (128/64 Bit) mit Passphrasen-/WEP-Schlüsselerstellung<br>Deaktivierung der SSID-Übertragung<br>Zugriffsbeschränkung nach MAC- und IP-Adressen |
| WEP-Schlüssel | 64 Bit, 128 Bit |
| Abmessungen | 140 mm x 140 mm x 27 mm |
| Gerätegewicht | 0,3 kg |
| Stromversorgung | 12 V WS, 1 A |
| Zertifizierungen | CE |
| Betriebstemperatur | 0 ºC bis 40 ºC |
| Lagertemperatur | -20 ºC bis 70 ºC |
| Betriebsfeuchtigkeit | 10 % bis 85 %, nicht kondensierend |
| Lagerfeuchtigkeit | 5 % bis 90 %, nicht kondensierend |

# Anhang I: Kontaktinformationen

Möchten Sie sich persönlich an Linksys wenden?
Informationen zu den aktuellen Produkten und Aktualisierungen für bereits installierte Produkte finden Sie online unter: http://www.linksys.com/international

Wenn Sie im Zusammenhang mit Linksys Produkten auf Probleme stoßen, können Sie uns unter folgenden Adressen eine E-Mail senden:

| In Europa | E-Mail-Adresse |
|---|---|
| Belgien | support.be@linksys.com |
| Dänemark | support.dk@linksys.com |
| Deutschland | support.de@linksys.com |
| Frankreich | support.fr@linksys.com |
| Großbritannien & Irland | support.uk@linksys.com |
| Italien | support.it@linksys.com |
| Niederlande | support.nl@linksys.com |
| Norwegen | support.no@linksys.com |
| Österreich | support.at@linksys.com |
| Portugal | support.pt@linksys.com |
| Schweden | support.se@linksys.com |
| Schweiz | support.ch@linksys.com |
| Spanien | support.es@linksys.com |

| Außerhalb von Europa | E-Mail-Adresse |
|---|---|
| Lateinamerika | support.la@linksys.com |
| USA und Kanada | support@linksys.com |